



RAS-PutIn Installation and User Guide

Based on Firmware 03.02.01

©Copyright 2003 Blackbox Inc.

All rights reserved

This publication contains proprietary information, which is protected by copyright. No part of this publication can be reproduced, transcribed, stored in a retrieval system, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, Blackbox Inc.. Blackbox Inc. acknowledges the following trademarks:

- Intel is a registered trademark of Intel Corporation.
- Windows 98, Microsoft Windows, and Windows NT are trademarks of Microsoft Corporation.
- IBM, AT, VGA, PS/2, and OS/2 are registered trademarks and XT and CGA are trademarks of International Business Machines Corporation.
- Blackbox is a registered trademark of Blackbox Inc. Zwickau, Germany.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Blackbox Inc. disclaims any proprietary interest in trademarks and trade names other than its own

Authors: Blackbox Team

This document was created on May 23, 2003.

The RAS-PutIn™ (ServSwitch RAS-PutIn) provides server management capabilities. You can use RAS-PutIn to manage and monitor components in your servers through a modem, an ISDN line or LAN, even if your network is down (Modem/ISDN). RAS-PutIn offers a comprehensive hardware solution to server management.

Limited Warranty

The buyer agrees if this product proves to be defective, that Blackbox Inc. is only obligated to repair or replace this product at Blackbox Inc.'s discretion according to the terms and conditions of the warranty registration card that accompanies this product. Blackbox Inc. shall not be held liable for any loss, expenses or damage, direct, incidental or consequential resulting from the use of this product. Please see the Warranty Information shipped with this product for full warranty details.

Limitations of Liability

Blackbox Inc. shall in no event be held liable for any loss, expenses or damages of any kind whatsoever, whether direct, indirect, incidental, or consequential (whether arising from the design or use of this product or the support materials provided with the product). No action or proceeding against Blackbox Inc. may be commenced more than two years after the delivery of product to Licensee of Licensed Software.

Licensee agrees to defend and indemnify Blackbox Inc. from any and all claims, suits, and liabilities (including attorney's fees) arising out of or resulting from any actual or alleged act or omission on the part of Licensee, its authorized third parties, employees, or agents, in connection with the distribution of Licensed Software to end-users, including, without limitation, claims, suits, and liability for bodily or other injuries to end-users resulting from use of Licensee's product not caused solely by faults in Licensed Software as provided by Blackbox Inc. to Licensee.

Technical Support

If you need help installing, configuring, or running RAS-PutIn, call your Blackbox OEM or VAD Technical Support representative.

We invite you to access Blackbox's Web site at:

<http://www.blackbox.com/>

There you shall find all modifications made after the editorial deadline.

Contents

1	The Quick Installation Guide	1
2	Introduction	5
2.1	When the server is up and running	7
2.2	When the server is dead	8
3	Installation	9
3.1	Operation Overview	9
3.2	Connectors and Jumpers	10
3.2.1	Front Side Connectors	10
3.2.2	Rear Side Connectors	10
3.3	Connecting RAS-PutIn to the host system	11
3.3.1	Connecting system management option	12
3.3.2	Connecting IPMI option	12
3.3.3	Connecting the Internal Reset/Power Option	13
3.3.4	Connecting the External Reset/Power Option	13
3.3.5	Connecting Ethernet	14
3.3.5.1	10 Mbps Connection	14
3.3.5.2	100 Mbps Connection	14
3.3.6	Connecting ISDN	14
4	Configuration	15
4.1	Initial Configuration	15
4.1.1	Initial configuration via DHCP server	15
4.1.2	Initial configuration via local console	15
4.1.3	Mouse, Keyboard and Video configuration	17
4.1.3.1	RAS-PutIn mouse settings	17
4.1.3.2	Host system mouse settings	17
4.1.3.3	RAS-PutIn Video Modes	17
5	Usage	19
5.1	Prerequisites	19
5.2	Login into RAS-PutIn and logout	20
5.2.1	Login into RAS-PutIn	20
5.2.2	Main Screen	21
5.2.3	Logout from RAS-PutIn	22
5.3	Remote Console	22
5.3.1	Show Remote Console	22
5.3.2	Remote Chat Frame	26
5.3.3	RAS-PutIn Mouse Synchronization	27
5.3.4	RAS-PutIn Video Settings	28

5.3.4.1	Video Settings through the HTML-Frontend	29
5.3.4.2	Video Settings through the remote console	29
5.3.4.3	Custom Video Modes	30
5.3.5	Remote Console Settings	31
5.3.6	Telnet Console	33
5.4	Server	34
5.4.1	Power Control	34
5.4.2	Keyboard/Mouse Settings	36
5.4.3	KVM Settings	37
5.5	Administration	39
5.5.1	User/Group Management	39
5.5.1.1	Add User	40
5.5.1.2	Delete User	40
5.5.1.3	Modify User	40
5.5.1.4	Copy User	40
5.5.1.5	Add Group	40
5.5.1.6	Delete Group	41
5.5.1.7	Modify Group	41
5.5.1.8	Copy Group	41
5.5.2	User/Group Permissions	41
5.5.3	Network Settings	42
5.5.3.1	Dynamic DNS	44
5.5.4	SNMP Settings	45
5.5.5	Serial Settings	47
5.5.6	Modem Settings	49
5.5.7	ISDN Settings	50
5.5.7.1	I want to allow non-callback dial in for everyone.	52
5.5.7.2	I want to allow non-callback dial in for selected people.	52
5.5.7.3	I want to allow non-callback dial in for everyone except some people that should be called back.	52
5.5.7.4	I want to allow non-callback dial in for selected people except some people that should be called back.	52
5.5.7.5	I want to allow callback connections only.	52
5.5.8	IPMI Settings	52
5.5.8.1	Generals	52
5.5.8.2	IPMI Settings	53
5.5.8.3	Power Control	54
5.5.8.4	Event Log via IPMI	54
5.5.8.5	Status via IPMI	54
5.5.9	LDAP Settings	55
5.5.9.1	Generals	55
5.5.9.2	LDAP Settings	55
5.5.10	Security Settings	56
5.5.10.1	SSL Settings	56
5.5.10.2	Telnet Settings	57
5.5.10.3	IP Access Control	58
5.5.11	SSL Certificate Management	59
5.5.12	Maintenance	60
5.5.12.1	Update Firmware	61
5.6	Access via Telnet	62

6	Frequently Asked Questions	65
A	Glossary	67
B	RAS-PutIn Video Modes	69
C	Key Codes	71
D	Pin Assignments	73
D.1	VGA HD-15	73
D.2	RJ 45 Connector Ethernet	73
D.3	RJ 45 Connector ISDN	74
D.4	Serial SUB-D 9 Connector 1	74
D.5	Serial SUB-D 9 Connector 2	74
D.6	KVM SUB-D 25 Connector	75
D.7	Power Supply Connector	75
E	Blackbox Warranty information	77
F	Specifications	79
F.1	Size and Weight	79
F.2	Environmental	79
G	Operation advices	81

List of Figures

1.1	Front Side Connectors	1
1.2	Rear Side Connectors	2
1.3	Top part of the Remote Console	4
2.1	RAS-PutIn total view	5
2.2	Internal Reset/Power Option - PC bracket	7
3.1	RAS-PutIn usage scenario	9
3.2	Multiple users on multiple servers	9
3.3	RAS-PutIn Front Side Connectors	10
3.4	Rear Side Connectors	10
3.5	Connections of RAS-PutIn KVM signals to the controlled system	11
3.6	Connections of RAS-PutIn with local console	12
3.7	Connecting RAS-PutIn system management	12
3.8	Top view of internal reset/power option	13
5.1	Internet Explorer showing the encryption key length	20
5.2	RAS-PutIn login screen	21
5.3	RAS-PutIn home menu window	22
5.4	Remote Console window showing a Windows 2000 desktop screen	23
5.5	Example for the Chat window	26
5.6	Video Settings in HTML frontend	29
5.7	Video Settings Panel	30
5.8	Custom Video Modes	31
5.9	Example of Remote Console settings	34
5.10	Telnet Console	34
5.11	Internal Power Control	35
5.12	External Power Control	36
5.13	Power Control via IPMI	36
5.14	Keyboard/Mouse settings	37
5.15	KVM Settings	38
5.16	User/Group Management	39
5.17	User/Group Permissions panel	41
5.18	RAS-PutIn network settings	43
5.19	Dynamic DNS Scenario	44
5.20	Dynamic DNS configuration panel	45
5.21	SNMP settings	46
5.22	Serial Settings	48
5.23	Internal Power Option Settings	49
5.24	RAS-PutIn ISDN settings panel	51
5.25	IPMI settings panel	53

5.26 IPMI Event Log	54
5.27 Example of IPMI State panel	55
5.28 LDAP settings panel	55
5.29 Security settings	57
5.30 SSL Certificate Request	60
5.31 SSL Certificate Signing Request	61
5.32 Panel for uploading a new firmware	62
5.33 Panel to update a new firmware that was previously uploaded	62
5.34 Maintenance	63
C.1 English (US) Keyboard Layout, used for key codes	71

List of Tables

1.1	Initial configuration	3
1.2	Serial parameters	3
2.1	Host system failures and how they are detected	8
4.1	Initial IP configuration	15
4.2	Serial line parameters	16
5.1	Meaning of the main menu RAS-PutIn features	23
5.2	Remote reset and power button effects	35
5.3	RAS-PutIn user and group permissions	42
5.4	Security parameters	56
5.5	Telnet security settings	57
B.1	RAS-PutIn Video Modes	69
C.1	Key Names	71

1 The Quick Installation Guide

Installation

RAS-PutIn redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted via IP. RAS-PutIn can be used in a multi administrator and multi server environment as well. Combining RAS-PutIn with a KVM switched matrix allows to access multiple remote servers over a single remote console.

Connectors

Front Side Connectors (Figure 1.1)

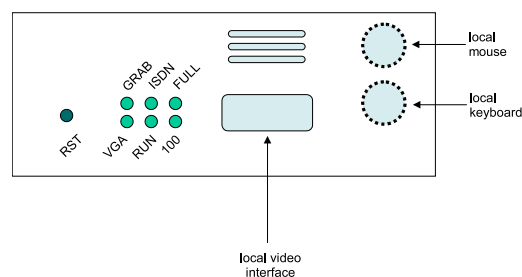


Figure 1.1: Front Side Connectors

Reset Pushing this button performs a reset of RAS-PutIn. The button is important for the initial configuration of RAS-PutIn

VGA Indicates, that the VGA input is active and a video signal is received by RAS-PutIn

RUN Indicates whether the RAS-PutIn system is running or not

100 Indicates that the Ethernet connection is in 100 Mbit mode

FULL Indicates that the Ethernet connection is in full-duplex mode

ISDN Indicates that the ISDN subsystem is available and active

GRAB Indicates that a remote user is logged onto RAS-PutIn and the video engine is outputting data

Using the connectors for video and keyboard/mouse a local console might be connected simultaneously.

Rear Side Connectors (Figure 1.2 on the next page)

SUB-D 9 Serial 1 The standard serial connector is used in multiple ways:

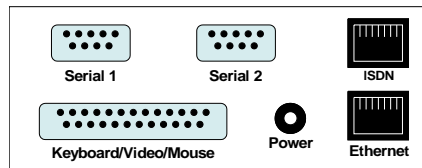


Figure 1.2: Rear Side Connectors

- IPMI Version 1.5 connection to the host system using the IPMI Option cable
- Serial output for modem dial in connection
- Serial pass-through via Telnet
- Initial configuration

SUB-D 9 Serial 2 The serial connector 2 supports the internal and external power options

SUB-D 25 KVM The supplied Keyboard VGA Mouse extender cable has an aggregated SUB D 25 connector to RAS-PutIn

Power supply A power supply with the following parameters must be attached:

- Voltage: 12 V
- Current: ≥ 1 A

RJ 45 ISDN Using this connector RAS-PutIn can be connected to an EURO ISDN network (EMEA versions only)

RJ 45 Ethernet UTP3/5 cables may be used to connect RAS-PutIn to an Ethernet LAN

Connecting RAS-PutIn to the host system

Perform the following steps in order to connect the KVM signals of the server system to RAS-PutIn:

1. Connect the SUB-D 25 to PS2/PS2/Video cable to the SUB-D 25 connector on RAS-PutIn
2. Connect the (purple) PS/2 Keyboard jack to the keyboard connector of the host system
3. Connect the (green) PS/2 mouse plug to the mouse connector of the host system
4. Connect the VGA HD-15 connector to the VGA monitor output of the host system
5. Connect the power supply as well as Ethernet and/or modem,ISDN, depending how you want to access RAS-PutIn

In case you want to connect a local console to the host system besides RAS-PutIn, you can attach monitor, keyboard and mouse to the according RAS-PutIn connectors on its front.

Video modes

RAS-PutIn recognizes a limited number of common video modes. When running X-Window on the host system, please don't use any custom modelines with special video modes. If done so,

RAS-PutIn may not be able to detect these. You are on the safe side with all standard VESA video modes. Please refer to Appendix B on page 69 for a list of all known modes.

Initial IP configuration

Initially the RAS-PutIn network interface is configured with the parameters shown in Table 1.1.

Table 1.1: Initial configuration

parameter	value
IP auto configuration	DHCP
IP address	192.168.1.22
Netmask	255.255.255.0
Gateway	none
IP access	disabled

If this initial configuration doesn't meet your local requirements, you need to do the initial IP configuration.

Use one of the following ways:

1. Connect the enclosed NULL modem cable to the serial interface on the RAS-PutIn rear side.

The serial interface needs to be adjusted with the parameters shown in table Table 1.2:

Table 1.2: Serial parameters

parameter	value
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

Use a terminal software (e.g. hyperterm or minicom) to connect to RAS-PutIn. Reset RAS-PutIn and immediately press < *ESC* >. You will see some device information and a '>' prompt. Enter the command 'config' and press < *Enter* >. After waiting a few moments you may configure IP auto configuration, IP address, net mask and default gateway. Pressing < *Enter* > without entering values does not change settings. The gateway value must be set to 0.0.0.0 (for no gateway) or any other value. You will be asked if the values are correct and get a chance to correct them. After confirming, RAS-PutIn performs a reset.

2. Use a crossover Ethernet cable to connect RAS-PutIn to your configuring computer back-to-back. Set the IP address of this computer to 192.168.1.1 and use the web interface with the initial IP configuration.

Web interface

RAS-PutIn may be accessed using a standard Web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of RAS-PutIn

into your Web browser. Initially there is only one user configured who has unrestricted access to all RAS-PutIn features:

Login name	super
Password	rasputin

Please login and change the password immediately according to your own policies.


The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system to which RAS-PutIn is attached. The Web browser which is used for accessing RAS-PutIn has to supply a Java Runtime Environment version 1.1 or higher. The Remote Console will behave exactly the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. Open the console by choosing the appropriate link in the navigation frame of the HTML frontend. Figure 1.3 shows the top of the Remote Console.



Figure 1.3: Top part of the Remote Console

There are some options to choose from, the important ones are the following:

Auto Adjust button 

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while RAS-PutIn tries to adjust itself for the best possible video quality.

Sync Mouse 

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general there is no need to change mouse settings on the host.

Video Settings in Options Menu This opens a new window with elements to control the RAS-PutIn Video Settings. You can change some values, for instance related to brightness and contrast of the picture displayed, which may improve the video quality. It is also possible to revert to the default settings for all video modes or only the current one.

2 Introduction

Features

RAS-PutIn defines a new class of remote KVM access devices (see Figure 2.1). RAS-PutIn ¹ combines digital remote KVM access via IP networks with comprehensive and integrated system management.

RAS-PutIn offers convenient, remote KVM access and control via LAN, Internet, or ISDN. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. RAS-PutIn provides a non-intrusive solution for remote access and control. Remote access and control software runs on the RAS-PutIn embedded processors only but not on mission-critical servers, so that there is no interference with server operation or impact on network performance.



Figure 2.1: RAS-PutIn total view

Furthermore, RAS-PutIn offers remote power management and remote system management according to the interfaces of the remote server. RAS-PutIn supports three ways of power management:

- via the internal reset/power option
- via external scalable power switch box
- via IPMI Version 1.5

¹RAS-PutIn— ServSwitch RAS-PutIn

Other features of RAS-PutIn are:

- KVM (keyboard, video, mouse) access over IP, ISDN or analogous telephone line.
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Port to connect a user console for direct analogous access to KVM switch
- Local Mouse suppression (only when using SUN's Java Virtual Machine)

RAS-PutIn supports consoles consisting of PS/2 style keyboards, PS/2 style mouse and HD 15 video output. Please refer to Appendix D.1 on page 73 for more details. RAS-PutIn will automatically detect the current video mode of the console, however manual fine tuning is recommended to receive the best video quality. RAS-PutIn will accept video streams up to 110 MHz dot clock. This results in a screen resolution of 1280x1024 dots with a frame rate of 60 Hz.

The used system management options depend on the interfaces the remote server systems provides. Three main system management options are offered:

IPMI Version 1.5	defines a serial connection to access certain system parameters and to perform system actions like powering down the system or performing a hard reset. Modern server systems, supporting the IPMI V1.5 specification, provide a mode where the externally available COM2 serial connection can be configured as system management port (sometimes also referred to as emergency management port). RAS-PutIn may use this port in order to enable remote system management operations.
Internal Reset/Power Option	The internal Reset/Power Option may be applied to remote systems where no IPMI Version 1.5 is available. The provided bracket is mounted in a free PCI/AGP slot. Main board pins for reset and power on/off have to be connected to the bracket. With this option it is possible to perform a remote reset, a remote power cycle, and a remote power on/off.
External Power Switch Option	In case there is neither an IPMI V1.5 option available nor the chance to place a bracket in the remote system, an external power switch box can switch the power on and off.

RAS-PutIn System Components

RAS-PutIn is a fully configured stand-alone product consuming one quart of a 1U 19" rack mount chassis space. Up to four RAS-PutIn devices can be mounted in 1 U chassis using the 19" rack mount kit (Item No: 8400200)

Each RAS-PutIn (Item No: 8400000) is shipped with:

1. RAS-PutIn base unit
2. Utility CD-ROM including
 - a) RAS-PutIn Installation and User Manual

- b) RAS-PutIn utilities
- 3. RAS-PutIn keyboard video mouse connection cable (Sub D 25)
- 4. NULL modem cable
- 5. RAS-PutIn external power supply

IPMI Option (Item No. 8400300) The IPMI Option consists of a serial cable (SUB-D 9 female ↔ SUB-D 9 female) for the connection between RAS-PutIn and an IPMI V1.5 compliant serial management port on the remote system.

Internal Reset/Power Option (Item No: 8400100) The internal reset/power option (see Figure 2.2) consists of a PC bracket with a Sub-D 9 jack on the outside and 4x2 pin connector in the inner side. The Sub-D 9 jack is connected to the RAS-PutIn Serial Port 2. The internal 4x2 pin connector allows to connect the reset and power on/off switching signals of the main board to RAS-PutIn. Figure 2.2 shows the PC bracket.



Figure 2.2: Internal Reset/Power Option - PC bracket

2.1 When the server is up and running

RAS-PutIn gives you full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and to send special commands to the server.

You can also perform periodic maintenance of the server. Using the Console Redirection Service, you are able to do the following:

- Reboot the system (a graceful shutdown).
- Watch the boot process.
- Boot the system from a separate partition to load the diagnostic environment.
- Run special diagnostic programs.

2.2 When the server is dead

Obviously, fixing hardware defects is not possible using a remote management device. Nevertheless RAS-PutIn gives the administrator valuable information about the type of a hardware failure.

Serious hardware failures can be categorized into five different categories with different chances to happen²:

- | | | |
|----|--|-----|
| 1. | Hard disk failure | 50% |
| 2. | Power cable detached, power supply failure | 28% |
| 3. | CPU, Controller, main board failure | 10% |
| 4. | CPU fan failure | 8% |
| 5. | RAM failure | 4% |

Using RAS-PutIn, administrators can determine which kind of serious hardware failure has occurred (see Table 2.1).

Table 2.1: Host system failures and how they are detected

Type of failure	Detected by
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remains in power off state after power on command has been given.
CPU Controller, main board failure	Power supply is on, but there is no video output.
CPU fan failure	By IPMI or server specific management software
RAM failure	Boot-Sequence on boot console

²According to a survey made by the Intel Corp.

3 Installation

3.1 Operation Overview

Figure 3.1 shows the connections of RAS-PutIn to its host, to peripheral devices, to the power source and to the local area network.

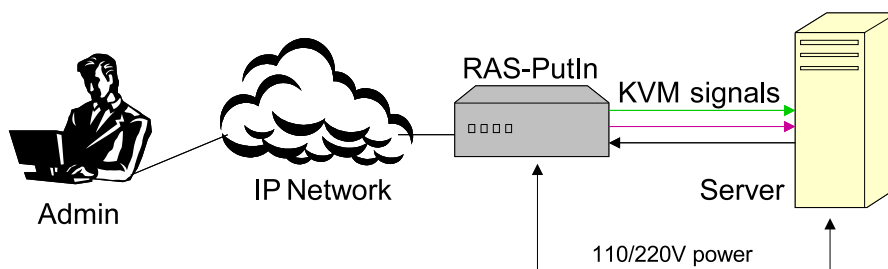


Figure 3.1: RAS-PutIn usage scenario

RAS-PutIn redirects local keyboard, mouse, and video data to a remote administration console. All data is transmitted via IP.

RAS-PutIn can be used in a multi administrator and multi server environment as well. Combining one or several RAS-PutIns with a KVM switched matrix allows to access multiple servers on a single remote console.

RAS-PutIn is multi user capable, i.e. up to 64 concurrent users may use RAS-PutIn to administer a remote site. Figure 3.2 shows a configuration with concurrent users on a number of servers connected by a KVM switching matrix using one or more RAS-PutIns.

Using more than one RAS-PutIn in a configuration as shown in Figure 3.2 prevents blocking administrators who use the switching matrix.

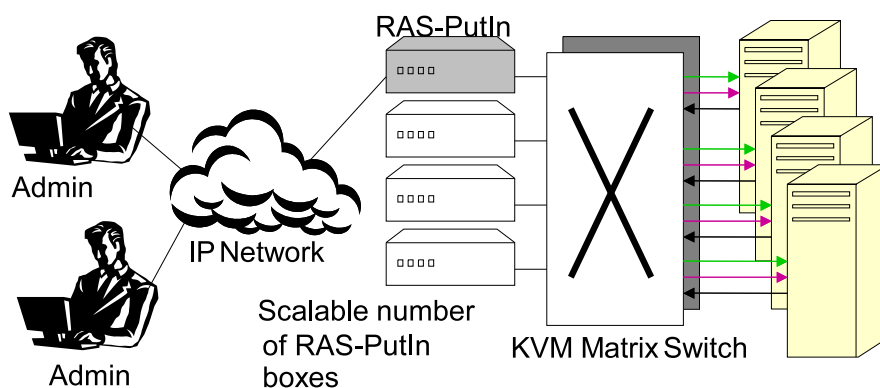


Figure 3.2: Multiple users on multiple servers

3.2 Connectors and Jumpers

3.2.1 Front Side Connectors

Figure 3.3 shows the connectors on RAS-PutIn's front side.

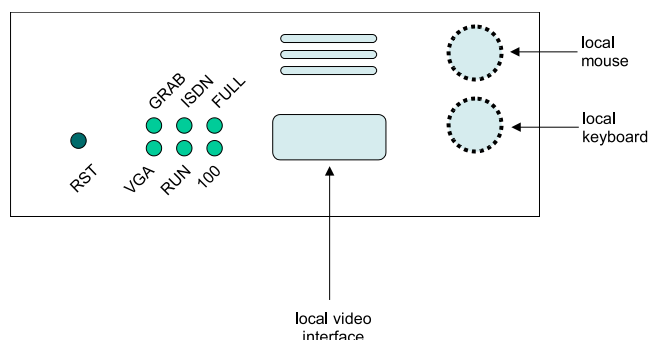


Figure 3.3: RAS-PutIn Front Side Connectors

- RST Pushing this button performs a reset of RAS-PutIn. One has to use this button for the initial configuration of RAS-PutIn
- VGA Indicates, that the VGA input is active and a video signal is received by RAS-PutIn
- RUN Indicates whether the RAS-PutIn system is running or not
- 100 Indicates that the Ethernet connection is in 100 Mbit mode
- FULL Indicates that the Ethernet connection is in full-duplex mode
- ISDN Indicates that the ISDN subsystem is available and active (EMEA version only)
- GRAB Indicates that a remote user is logged onto RAS-PutIn and the video engine is outputting data

In case you want to connect a local console to the host system besides RAS-PutIn, you can attach monitor, keyboard and mouse to the according RAS-PutIn connectors on its front.

3.2.2 Rear Side Connectors

Figure 3.4 shows the connectors on RAS-PutIn's rear side.

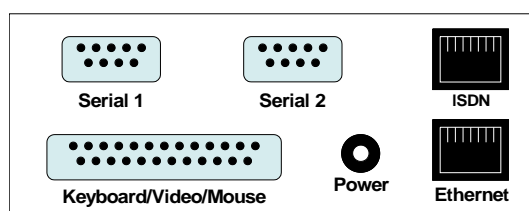


Figure 3.4: Rear Side Connectors

SUB-D 9 Serial 1 The standard serial connector is used in multiple ways:

- IPMI Version 1.5 connection to the remote system using the IPMI Option cable
- Serial output for modem dial in connection
- Serial pass-through via Telnet
- Initial configuration

SUB-D 9 Serial 2 The serial connector 2 supports the internal and external power options

SUB-D 25 KVM The supplied Keyboard VGA Mouse extender cable has an aggregated SUB D 25 connector to RAS-PutIn

Power supply A power supply with the following parameters can be attached:

- Voltage: 12 V
- Current: ≥ 1 A

RJ 45 ISDN Using this connector RAS-PutIn can be connected to an EURO ISDN network

RJ 45 Ethernet UTP3/5 cables can be connected to RAS-PutIn using this standard RJ 45 Jack

3.3 Connecting RAS-PutIn to the host system

In order to connect the KVM signals of the host system to RAS-PutIn perform the following steps:

1. Connect the SUB-D 25 to PS2/PS2/Video cable to the SUB-D 25 connector on RAS-PutIn
2. Connect the (purple) PS/2 Keyboard jack to the keyboard connector of the host system
3. Connect the (green) PS/2 mouse plug to the mouse connector of the host system
4. Connect the VGA HD-15 connector to the VGA monitor output of the host system
5. Connect the power supply as well as Ethernet and/or modem,ISDN, depending how you want to access RAS-PutIn

In case you want to connect a local console to the host system besides RAS-PutIn you may attach monitor, keyboard and mouse to the connectors on the front side. Figure 3.5 shows the resulting connections from RAS-PutIn to the host system, whereas Figure 3.6 on the next page shows the same connections including the local console ones.

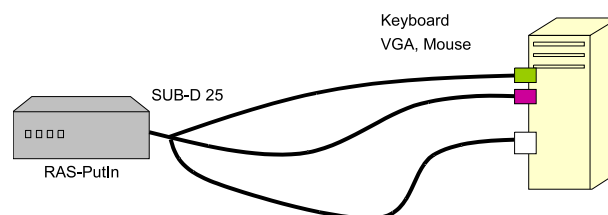


Figure 3.5: Connections of RAS-PutIn KVM signals to the controlled system

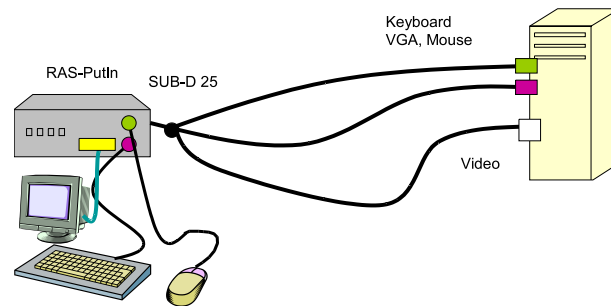


Figure 3.6: Connections of RAS-PutIn with local console

3.3.1 Connecting system management option

Figure 3.7 gives an overview over the three different options to perform remote reset and remote power management to the controlled PC.

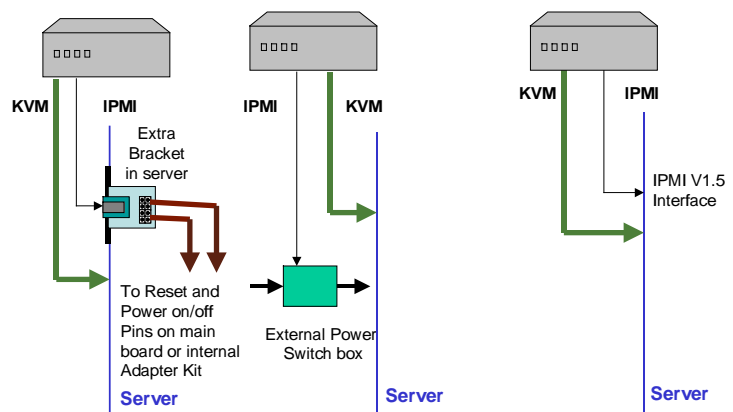


Figure 3.7: Connecting RAS-PutIn system management

3.3.2 Connecting IPMI option

IPMI Version 1.5 defines a serial connection to access certain system parameters and to perform system actions like powering down the system or performing a hard reset. Modern server systems, supporting the IPMI V1.5 specification, provide a modus where the externally available COM2 serial connection can be configured as system management port (sometimes also referred to as emergency management port). RAS-PutIn may connect to this port in order to enable remote system management operations.

At <http://developer.intel.com/design/servers/ipmi/index.htm> You will find further information about IPMI 1.5.

In order to use the IPMI over serial interface it has to be enabled in the host system. This can be done using BIOS settings or special utilities provided by the server manufacturer. Refer to the server manufacturer's manual site to find out how the IPMI over serial line can be enabled and configured and where the IPMI serial port is placed.

Hint:

IPMI V1.5 is only supported by modern server systems. No server system manufactured before 2002 supports IPMI 1.5. By the date of printing this manual only the Intel SDS2 server main board has a proper support of IPMI Version 1.5.

Connect the IPMI option serial cable to the RS232 port 1 on the rear side of RAS-PutIn and to the serial port of the controlled system.

3.3.3 Connecting the Internal Reset/Power Option

Figure 3.8 shows the top view of the reset/power bracket.

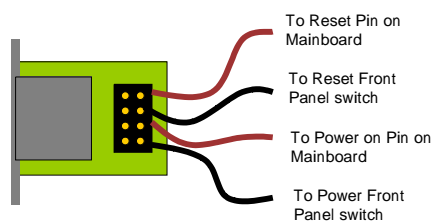


Figure 3.8: Top view of internal reset/power option

Additional cables are required in order to enable the remote reset and the remote power function of RAS-PutIn:

1. Mount the reset/power bracket in a free slot of the controlled system.
2. Find the cable connecting the front panel reset button and the main board.
3. Disconnect this cable from the main board and connect it to the pin connector on the bracket as shown in Figure 3.8.
4. Take the supplied red/black reset cable and connect the cable with one end to the main boards reset jumper connector (where you just disconnected the cable to the front panel) and with the other end to the bracket connector as shown in Figure 3.8.
5. Find the cable connecting the front panel power button and the main board.
6. Disconnect this cable from the main board and connect it to the pin connector on the bracket as shown in Figure 3.8.
7. Take the supplied red/black power cable and connect the cable with one end to the main board's power jumper connector (where you just disconnected the cable to the front panel) and with the other end to the bracket connector as shown in Figure 3.8.
8. Check the cabling: finally, there are four cables connected to the jumper connector on the bracket.

Now, connect the bracket to the RAS-PutIn serial port 2 using the supplied SUB-D 9 to SUB-D 9 connector.

3.3.4 Connecting the External Reset/Power Option

Please refer to the manual of the Blackbox external power switch option or a third party external power option to connect those external devices to one of the serial interface on the rear side of

RAS-PutIn. By the date of printing this manual supported options are:

- Avocent™SPC¹ 800/1600
- Sentry In-Line Power Module
- Leuning ePowerSwitch

3.3.5 Connecting Ethernet

The rear side of RAS-PutIn provides a RJ-45 connector for Ethernet. The connector is used either for a 100 Mbps 100BASE-TX connection or for a 10 Mbps 10BASE-T connection. The adapter can sense the connection speed and will adjust to the appropriate operation mode automatically.

3.3.5.1 10 Mbps Connection

For 10BASE-T Ethernet networks, the Fast Ethernet adapter uses Category 3, 4, or 5 UTP cable. To establish a 10 Mbps connection, the cable must be connected to a 10BASE-T hub.

1. Make sure that the cable is wired appropriately for a standard 10BASE-T adapter.
2. Align the RJ-45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

3.3.5.2 100 Mbps Connection

For 100BASE-TX Fast Ethernet networks, RAS-PutIn supports Category 5 UTP cabling. To establish a 100 Mbps connection, the cable must be connected to a 100BASE-TX hub.

1. Make sure that the cable is wired appropriately for a standard 100BASE-TX adapter.
2. Align the RJ-45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

Note:

The UTP wire pairs and configuration for 100BASE-TX cable are identical to those for 10BASE-T cable when used with Category 5 UTP cable.

3.3.6 Connecting ISDN

The rear side of RAS-PutIn contains two RJ-45 connectors. The upper connector, marked as 'ISDN' is used to connect RAS-PutIn to an ISDN network, using a standard ISDN cable.

¹Avocent is a registered trademark of Acovent Corp. Huntsville

4 Configuration

4.1 Initial Configuration

RAS-PutIn's communication interfaces are all based on TCP/IP. RAS-PutIn comes pre-configured with the IP configuration listed in Table 4.1.

Table 4.1: Initial IP configuration

Parameter	Value
IP auto configuration	DHCP
IP-Address	192.168.1.22
Net-mask	255.255.255.0
Default-Gateway	none
IP access control	disabled

In case this initial configuration doesn't meet your requirements there is an initial IP configuration necessary in order to access RAS-PutIn for the first time. This chapter describes different possibilities to accomplish that.

4.1.1 Initial configuration via DHCP server

By default, RAS-PutIn will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found it may provide a valid IP address, gateway address and net mask. Before you connect the RAS-PutIn to your local subnet be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of RAS-PutIn. You can find the MAC address of your RAS-PutIn on the outside of the shipping box and labelled on RAS-PutIn's bottom side. If the DHCP connection fails on boot up, RAS-PutIn will boot with the last known IP configuration. This is the pre-configured IP address in case RAS-PutIn is booting up for the very first time.

4.1.2 Initial configuration via local console

There are two ways for getting access to RAS-PutIn's local console and carrying out the IP configuration there:

1. Using a serial terminal: RAS-PutIn has a serial line interface at its rear side (refer to Section 3.2 on page 10). The connector is compliant to RS 232 serial line standard. We are offering an according serial cable that can be used for connecting the connector of RAS-PutIn with a Sub-D 9 connector of a terminal or the serial line interface of a computer running a terminal program. The serial line has to be configured with the parameters given in Table 4.2 on the following page.

2. Use a crossover Ethernet cable to connect RAS-PutIn to your configuring computer back-to-back and use the initial configuration to connect.

Table 4.2: Serial line parameters

Parameter	Value
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

When using the configuration with a serial terminal, reset RAS-PutIn and immediately press ESC. You will see some device information and a '=' prompt. Enter 'config', press < Enter > and wait a few seconds for the configuration questions to appear.

As you go along you will see the following lines, which you have to answer or to which you may provide the default value by pressing < Enter >. The default value is shown in square brackets.

IP auto configuration (none/dhcp/bootp) [dhcp]:

IP [192.168.1.22]:

NetMask [255.255.255.0]:

Gateway (0.0.0.0 for none) [0.0.0.0]:

Enable IP Access Control (yes/no) [no]:

- **IP autoconfiguration**

With this option you can specify whether RAS-PutIn should fetch it's network settings from a DHCP or BOOTP server. For DHCP you have to enter *dhcp* and for BOOTP supply *bootp* accordingly. If you specify *none* then IP autoconfiguration is disabled and you will subsequently be asked for the following network settings.

- **IP address**

The IP address the RAS-PutIn should use. This option is only available if IP autoconfiguration is disabled.

- **Subnet mask**

The mask of the connected IP subnet. This option is only available if IP autoconfiguration is disabled.

- **Gateway address**

The IP address of the default router of the connected IP subnet. If you have no default router, you may enter *0.0.0.0*. This option is only available if IP autoconfiguration is disabled.

- **Enable IP Access Control**

The last question 'Enable IP Access Control' allows you to switch IP packet filtering on or off. It is mainly intended to re-enable access to RAS-PutIn after a faulty IP access control configuration has been activated. Refer to Section 5.5.10.3 on page 58 for more information about IP access control.

There may be default values which are enclosed in brackets. If you want to use the default value of an option then you just need to press the *Enter* key.

You will be asked if the values are correct and get a chance to correct them. After confirming, RAS-PutIn performs a reset.

4.1.3 Mouse, Keyboard and Video configuration

The correct operation of the remote mouse depends on two settings which will be discussed in the following subsections. In case the remote mouse doesn't work properly at least one of the following settings is probably not correct.

4.1.3.1 RAS-PutIn mouse settings

The RAS-PutIn settings for the host's mouse type and the host's keyboard type must be correct in order to make remote keyboard and mouse work properly. Check the settings in the RAS-PutIn front-end. See Section 5.4.2 on page 36 for details.

4.1.3.2 Host system mouse settings

The host's operating system also knows various settings for the mouse driver. While RAS-PutIn works with accelerated mice and is able to synchronize the local with the remote mouse pointer (see Section 5.3.3 on page 27), there are the following limitations which may prevent this synchronization from working properly:

- | | |
|--------------------------|--|
| Special Mouse Driver | There are mouse drivers, which influence the synchronization process leading to desynchronized mouse pointers. If this happens, make sure you don't use a special vendor-specific mouse driver on your host system |
| Windows XP Mouse Setting | Windows XP knows a setting to 'improve mouse acceleration', which has to be deactivated |

You can check the correct setting by moving the mouse of your administration system to the upper left corner of the Remote Console and moving it there slightly forth and back. This will force a mouse synchronization in that corner of the screen. Once that is done you may observe the behaviour of your remote mouse in accordance to the local one. If both mice desynchronize quickly one of the above mentioned settings may be not correct.

4.1.3.3 RAS-PutIn Video Modes

RAS-PutIn recognizes a limited number of common video modes. When running X-Window on the host system, please don't use any custom modelines with special video modes. If done so, RAS-PutIn may not be able to detect these. You are on the safe side with all standard VESA video modes. Please refer to Appendix B on page 69 for a list of all known modes.

5 Usage

5.1 Prerequisites

The RAS-PutIn features an embedded operating system and the according applications offering a variety of standardized interfaces. The functionality is exposed to the user via these interfaces. This chapter will describe all of these interfaces and how to use them in detail. All the interfaces are accessed using the TCP/IP protocol family, thus they can be used equally over the built-in Ethernet adapter , over modem or over ISDN.

The following interfaces are supported:

1. HTTP/HTTPS: The most complete access is provided by an embedded Web server. Thus the RAS-PutIn environment can be entirely controlled by a standard Web browser. Depending on the Web browser you can access the RAS-PutIn card using the unsecured HTTP protocol or, in case the browser supports it, the encrypted HTTPS protocol. It is recommended to use HTTPS whenever possible.
2. SNMP¹: Any standard SNMP client can use this protocol. The according MIB² is provided on the RAS-PutIn tools CD or can be downloaded over the RAS-PutIn front-end.
3. Telnet: A standard Telnet client can be used to access an arbitrary device connected to RAS-PutIn's serial port via a terminal mode.

Since the primary interface of RAS-PutIn is the HTTP interface this chapter is mainly concerning this topic. Other interfaces are explained in their according subtopics.

In order to use the Remote Console window of your managed host system the browser has to come with a Java Runtime Environment version 1.1 or higher. But even if the used browser has no Java support, for instance on small handheld devices, you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

We recommend the following browser for an unsecured connection to RAS-PutIn.

- Microsoft Internet Explorer version 5.0 or higher on Windows 98, Windows ME and Windows 2000, Windows XP
- Netscape Navigator 7.0 or Mozilla 1.0 on Windows 98, Windows ME, Windows 2000, Windows XP, Linux and other UNIX like Operating Systems

In order to access the remote host system using a securely encrypted connection you need a browser that supports the HTTPS protocol. Strong security is only assured by using key length of 128 Bit. Many old browsers don't have a strong 128 Bit encryption algorithm due to former export regulations of US authorities. For instance Internet Explorer 5.0, that comes as part of Windows ME and Windows 2000 supports a key length of 56 Bit only. You can read about the key length of your Internet Explorer under the menu points '?' and 'Info'. The dialog box

¹SNMP — Simple Network Management Protocol

²MIB — Management Information Base

shows also a hyperlink that leads you to information on how to upgrade your browser to a state of the art encryption scheme. Figure 5.1 shows the dialog presented by Internet Explorer 6.0.

However the US export regulations have been declared obsolete recently. Therefore, new browser versions do support strong encryption.

We recommend the following browser for a secured connection to RAS-PutIn.

- Microsoft Internet Explorer version 5.5 or higher on Windows 98, Windows ME and Windows 2000 and Windows XP
- Netscape Navigator 7.0 or Mozilla 1.0 on Windows 98, Windows ME, Windows 2000, Windows XP, Linux and other UNIX like Operating Systems



Figure 5.1: Internet Explorer showing the encryption key length

5.2 Login into RAS-PutIn and logout

5.2.1 Login into RAS-PutIn

Start your Web browser and direct it to the address of your RAS-PutIn that has been configured during installation. The address used might be a plain IP address or a host and domain name, in case you have given your RAS-PutIn a symbolic name in the DNS.

For instance, you have to type the following into the address line of your browser for establishing an unsecured connection:

`http://192.168.1.22/`

or in case you like to use a secure connection:

`https://192.168.1.22/`

This leads you to the RAS-PutIn login page as shown in Figure 5.2 on the facing page.

The RAS-PutIn has a built-in super user that has all permissions to administrate your RAS-PutIn:

Login name	super
Password	rasputin



Figure 5.2: RAS-PutIn login screen

Attention:

Please make sure to change the super user password immediately after you have installed and firstly accessed your RAS-PutIn. Not changing the super user password is a severe security risk and might result in unauthorized access to RAS-PutIn and the host system with all possible consequences!

5.2.2 Main Screen

After a successful login, RAS-PutIn will present its main screen consisting of three frames (see Figure 5.3 on the next page)

The upper left frame contains a home link that brings you instantly back to the home page after you stepped down to one of the administration menu points. The logout link logs you out of RAS-PutIn. That means the current session will be terminated and you have to type username and password again to login.

Note:

The RAS-PutIn will log you out automatically after there is no administration activity for half an hour. In this case each click on one of the links will lead you to the login screen where you have to provide the login information again.

The lower left frame of the RAS-PutIn main window, called the menu frame, contains the main menu that leads you to the pages for various administration tasks. The functions of the menu frame will be described in detail during the following sections.

The different function pages selected by one of the menu links will be presented in the big right frame, called the function frame.

Initially the function frame contains a short summary of your RAS-PutIn. Table 5.1 on page 23 gives you a description of the meaning of each point.

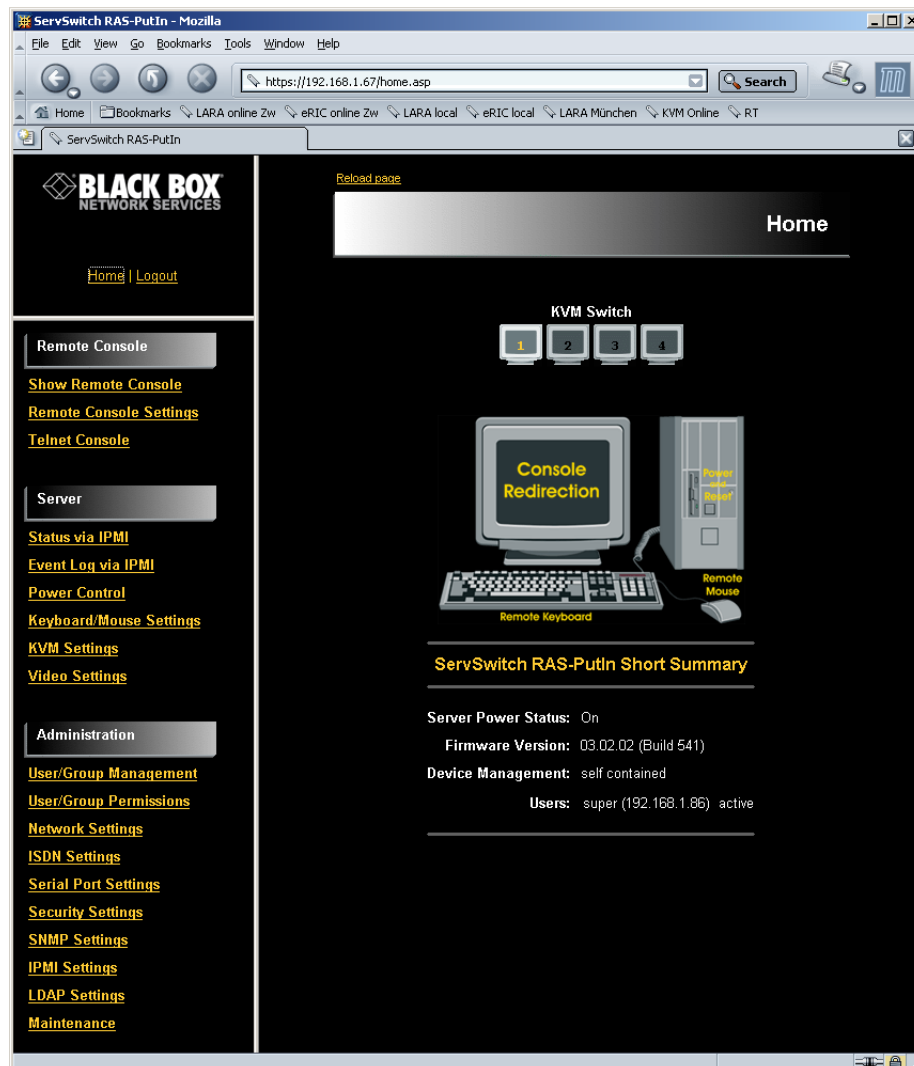


Figure 5.3: RAS-PutIn home menu window

5.2.3 Logout from RAS-PutIn

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed in case there is no activity for half an hour.

5.3 Remote Console

5.3.1 Show Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system RAS-PutIn controls.

Starting the Remote Console causes an additional window popping up that contains a copy of the screen of your host system (see Figure 5.4 on the next page). The Remote Console will behave exactly in the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However,

Table 5.1: Meaning of the main menu RAS-PutIn features

Feature	Description
Server Power Status	Shows whether the host system is switched on or off
Firmware Version	Version number of the firmware installed on your RAS-PutIn
Device Management	Shows, if RAS-PutIn is entirely self-managed or if its connected to a management device.
Users	Shows all currently logged in users with their identity and the IP address from where they are logged in (note: in case a user connected his Web browser over a proxy server the IP address field will show the IP address of the proxy server and not that of the user machine itself). RC means that the user has opened the Remote Console. Exclusive is a sign that the Remote Console is opened in exclusive mode. Idle is the time since last access during the current session.

be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the line over which you are connected to RAS-PutIn.

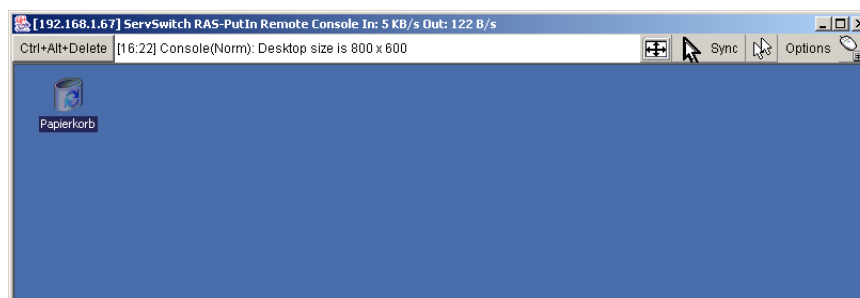


Figure 5.4: Remote Console window showing a Windows 2000 desktop screen

With respect to the keyboard, the very exact remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the remote host system.

For instance, special keys on the German keyboard won't work anymore as expected but will result in their US English counterpart if you are using a German administration system but your host system uses a US English keyboard layout.

You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one or by using the Soft-Keyboard that is part of the Remote Console applet.

The Remote Console window is a Java Applet that tries to establish its own TCP connection to RAS-PutIn. The protocol that is run over this connection is not HTTP or HTTPS but a protocol called RFB (Remote Frame Buffer Protocol). Currently RFB tries to establish a connection to port number 443. Your local network environment must allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings must be configured accordingly.

In case RAS-PutIn is connected to your local network environment and your connection to

the internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the according connection. This is because today's Web proxies are not capable of relaying the RFB protocol.

In case of problems, please consult your network administrator in order to provide an appropriate network environment.

The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

Hint:

In difference to the remote host system, the Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus.

The upper part of the Remote Console window contains a control bar. Using its elements you can see the state of the Remote Console and influence the local Remote Console settings. Section 5.3 on page 22 describes the meaning of each control.

Description of Remote Console Options

- **Ctrl+Alt+Delete**

Special button key to send the 'Control Alt Delete' key combination to the remote system (see also Section 5.3.5 on page 31 for defining new button keys).

- **State line**

Shows console and connection state. Normally it displays the size of the remote screen in pixels. The value in round brackets describes the connection to the remote system: Norm stands for a standard connection without encryption; SSL stands for a secured connection. In case there is a connection error, it will be displayed in this line as well. You can double click the state line in order to see a history of all the state messages.

- **Auto adjust**



Starts the auto adjustment procedure to determine the settings for best visual quality of the grabbed image. This may take a few moments. During the process the display is turned off and you will see a notification message.

- **Sync mouse**



Activates the mouse synchronization process. Have a look at Section 5.3.3 on page 27 for further information about this topic.

- **Single/Double mouse mode**



Switches between the Single Mouse Mode (where only the remote mouse pointer is visible)

and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.3 or higher.

- **Monitor Mode**



Toggles the read only mode on and off. In case the Monitor Mode check box is checked the Remote Console won't accept any local input neither keyboard nor mouse. The symbol shows if the monitor mode is currently active or not.

- **Options**

- **Exclusive Access**

If a user has the appropriate permission, he can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

- **Options**

- **Scaling**

Allows you to scale down the Remote Console. You can still use mouse and keyboard, however the scaling algorithm won't preserve all display details.

- **Options**

- **Readability Filter**

Toggles the Readability Filter on or off. If the filter is switched on in scaling mode, it will preserve most of the screen details even if the image is substantially scaled down. This option will be available only with a Java Virtual Machine version number of 1.3 or higher.

- **Options**

- **Chat Window**

Opens up the RAS-PutIn Chat Frame. See Section 5.3.2 on the next page for a detailed description!

- **Options**

- **Soft Keyboard**

Opens up the Menu for the Soft-Keyboard.

- **Options**

- **Soft Keyboard**

- **Show**

Pops up the Soft-Keyboard. The Soft-Keyboard is necessary in case your host system runs a completely different language and country mapping than your administration machine.

- **Options**

- **Soft Keyboard**

- **Mapping**

Used for choosing the according language and country mapping of the Soft-Keyboard.

- **Options**

- **Local Keyboard**

Used to change the language mapping of your browser machine running the Remote Console Applet. Normally the Applet determines the correct value automatically. However, depending on your particular JVM and your browser machine settings this is not always possible. A typical example is a German localized system that uses an US-English keyboard mapping. In this case you have to change the Local Keyboard setting manually to

the right language

- **Options**

- **Video Settings**

Opens a panel for changing the RAS-PutIn video settings. Have a look at Section 5.3.4 on page 28 for a detailed description of the available options.

- **Options**

- **Mouse handling**

The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointer, explained in Section 5.3.3 on the next page. The option for 'Fast Sync' shows the hotkey in parentheses in case you defined one using the Remote Console Settings. It is also possible to activate the 'Exclusive Mouse Mode' (see Section 5.3.5 on page 31 for an explanation).

- **Options**

- **Local cursor**

Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated again next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine, only a version of 1.2 or higher offers the full list.

The Remote Console title bar shows some information about the incoming ('In:') and outgoing network traffic ('Out:').

If you are using the compressed encoding, compressed and uncompressed incoming traffic will be shown.

5.3.2 Remote Chat Frame

The RAS-PutIn Remote Console features a Chat Frame that allows you to communicate with other parties logged into the same device. Figure 5.5 shows an example of the Chat Frame.

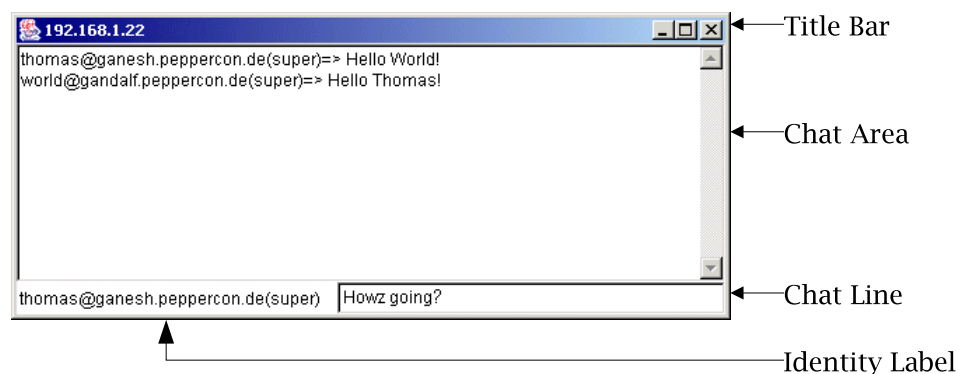


Figure 5.5: Example for the Chat window

The Chat Frame is helpful especially for discussing problems and questions among logged in RAS-PutIn users in case the remote host's screen should not be changed or misused for that purpose.

Below all Chat Frame elements are listed together with their meaning and usage. The elements will be referred to by the terms introduced in Figure 5.5.

Chat Frame element description

- **Title Bar**
Shows the IP address of the RAS-PutIn you are connected to.
- **Chat Area**
Read-only text area showing the messages, which have been received so far, inclusive your own messages sent to others. The identity string of the sender precedes each message.
- **Identity Label**
Shows the identity string used to precede messages sent by this Chat Frame. The first part of the identity string is the user ID that has been used to log into the client system, i.e. the system the browser runs on. The second part, behind '@', is the hostname of the client system. The last part in round brackets is the user name that was used to log into RAS-PutIn ('super' in the example).
- **Chat Line**
This is an editable text line, where a new message can be entered. Once the Enter key is hit the message is broadcasted to every other connected party. In case a connected user has not yet opened the Chat Frame it will be opened automatically in order to deliver the message.

Note:

Any message sent to the Chat will be broadcasted to ALL connected users, which are using the Remote Console at the time the message was sent. There is no option to direct a message to a particular user only.

The Chat has no message history. That means, messages will be received only after opening the Remote Console. Messages that possibly have been sent among other users will be lost for a user who opens up his Remote Console afterwards.

5.3.3 RAS-PutIn Mouse Synchronization

Introduction A common problem with KVM devices is the synchronization between the local and remote mouse cursors. RAS-PutIn addresses this situation with an intelligent synchronization algorithm. There are two mouse modes available on RAS-PutIn.

Direct Mode This mode just translates the mouse movements from the Remote Console in a way that one pixel move will lead to 'n' pixel moves on the remote system. This parameter 'n' is adjustable with the scaling. The direct mode works only when mouse acceleration is turned off on the remote system.

Automatic Mode The automatic mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.

Automatic mode and mouse synchronization The automatic mode performs the speed detection during mouse synchronization. Whenever the mouse doesn't move correctly, there are two ways for re-synchronizing local and remote mouse:

Fast Sync The fast synchronization is used to correct a temporary, but fixed skew. Choose the option using the Remote Console options menu (see Section 5.3 on page 22) or press the mouse synchronization hotkey sequence in case you defined one (refer to Section 5.3.5 on page 31).

Intelligent Sync If the fast sync doesn't work or the mouse settings have been changed on the host system, use the intelligent resynchronization. This method takes more time than the fast one and can be accessed with the appropriate item in the Remote Console option menu. The intelligent synchronization requires a correctly adjusted picture. Use the auto adjustment function or the manual correction in the Video Settings panel (refer to Section 5.3.4) to setup the picture.

The 'Sync mouse' button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a fast sync, except in situations where the KVM port or the video mode changed recently.

Limitations of the mouse synchronization While the intelligent algorithm works fine for common cases, there are some special limitations which may prevent the synchronization from working properly:

Special Mouse Driver	There are mouse drivers, which influence the synchronization process leading to desynchronized mouse pointers. If this happens, make sure you don't use a special vendor-specific mouse driver on your host system
Windows XP Mouse Setting	Windows XP knows a setting to 'improve mouse acceleration', which has to be deactivated
Badly adjusted picture	To have the intelligent sync working, a correctly adjusted picture is necessary. Use the auto adjustment function or the manual correction in the Video Settings panel (refer to Section 5.3.4) to setup the picture. The video also has to be of sufficiently good quality.
Active Desktop	Check if you have the Active Desktop feature of Microsoft Windows enabled. If so, don't use a plain background, use some kind of wallpaper. You could also disable the Active Desktop entirely.

Single and Double Mouse Mode The information above applies to the *Double Mouse Mode*, where remote and local mouse pointers are visible and need to be synchronized. RAS-PutIn also features another mode, the *Single Mouse Mode*, where only the remote mouse pointer is visible. Activate this mode in the open Remote Console (see Section 5.3 on page 22) and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode, it is necessary to define a mouse hotkey in the Remote Console Settings Panel (Section 5.3.5 on page 31). Press this key to free the captured local mouse pointer.

Single Mouse mode needs at least a Sun Java Virtual Machine 1.3

5.3.4 RAS-PutIn Video Settings

RAS-PutIn features two different dialogs which influence the video settings.

5.3.4.1 Video Settings through the HTML-Frontend

One side is the video options panel in the RAS-PutIn HTML-Frontend (see Figure 5.6)

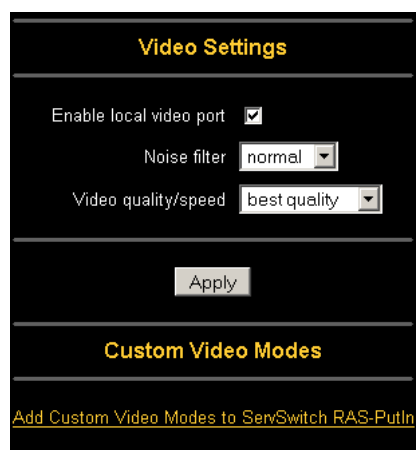


Figure 5.6: Video Settings in HTML frontend

Enable local video port: This option decides if the local video output of RAS-PutIn is active and passing through the incoming signal from the host system.

Noise filter: This option defines how RAS-PutIn reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Video Quality and Speed: Using this option it is possible to tune the video system of RAS-PutIn to either maximize picture quality or speed. When set to 'best quality' the picture looks clean but the video update speed won't be as fast as possible. If responsiveness is more important to you than achieving the best quality, set the option to 'high speed'. In this mode, artifacts will appear. An intermediate setting is also available. Please note that the difference is only clearly visible when using fast network links and the normal compression for the Remote Console.

5.3.4.2 Video Settings through the remote console

RAS-PutIn features a panel to setup the following video options (see Figure 5.7 on the following page), available in the Remote Console Options menu.

Brightness	Controls the brightness of the picture
Black level	Defines what intensity of color is still recognized as black
Contrast	Controls the contrast of the picture
Clock	Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjunction with the auto adjustment procedure should be adequate for all common configurations. If the picture quality is still bad after auto adjustment you may try to change this setting together with the sampling phase to achieve a better quality.

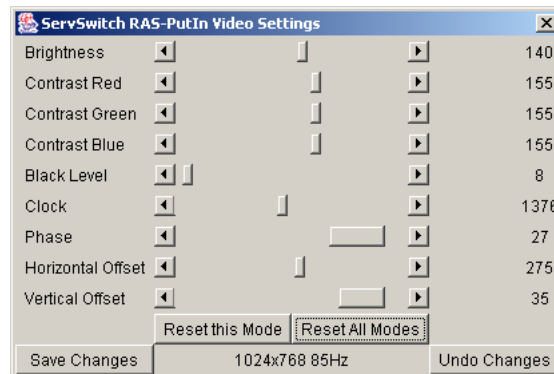


Figure 5.7: Video Settings Panel

Phase	Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.
Horizontal Position	Use the left and right buttons to move the picture in horizontal direction while this option is selected
Vertical Position	Use the left and right buttons to move the picture in vertical direction while this option is selected
Reset this Mode	Resets mode specific settings to their factory defaults
Reset all Modes	Resets all settings to their factory defaults
Save changes	Save changes permanently
Undo changes	Restore last settings

Brightness, Black level and Contrast affect all modes and KVM ports globally, the other settings are changed specifically for each mode on each KVM port.

Video Settings Permissions Video settings are divided into two parts with different permissions. An user of the Remote Console which has the 'standard' permission is able to change Brightness, Contrast, Black level and the picture positions. The 'advanced' permission allows to additionally change Clock, Phase and to use the reset buttons.

5.3.4.3 Custom Video Modes

Using this option (see Figure 5.8 on the next page) it is possible to add video modes to RAS-PutIn, which are not recognized using the factory settings. This may be useful when using special modelines in a X-Window configuration on the host or with uncommon hosts or operating systems.

This option is for advanced users only, it is possible to influence the correct video transmission by using this option, so use it with care!

The maximum number of custom video resolutions is 4. Using the option "Custom Modes Handling" custom modes may be disabled ("Off"), used additional to the standard video resolutions or used exclusive ("Only"). With the last option it is also possible to force a special video mode for RAS-PutIn.

Figure 5.8: Custom Video Modes

To change the parameters for a mode, choose the number and press "Update". It is necessary to provide some information so the video mode may be correctly recognized:

- **X Resolution**
Visible number of horizontal pixels.
- **Y Resolution** Visible number of vertical pixels.
- **Horizontal Frequency (Hz)** The horizontal (line) frequency in Hz.
- **Vertical Frequency (Hz)** The vertical (refresh) frequency in Hz.
- **Total horizontal pixels** The total amount of pixels per line, including the non-visible and blanking area.
- **Polarity** The polarity (positive/negative) of the synchronization signals. V means vertical, H means horizontal.
- **Description** Here you can provide a mode name which is displayed in the Remote Console if this custom mode is activated.

5.3.5 Remote Console Settings

The Remote Console settings allow you to customize the Remote Console window prior to its start (see Figure 5.9 on page 34). Some of the parameters you might still change while the Remote Console is running while others have to be set in the Remote Console settings.

All the settings for the Remote Console window are user specific. That means, each user can individually customize the Remote Console for his needs. Changing the settings for one user does not affect the settings for others.

- **User select box**
This control will show the user ID for which the values are shown and for which changes will take effect. You might change the settings of other users in case you have the necessary access rights.
- **Transmission Encoding**
The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. Using those settings it is possible to optimize the speed of the remote screen depending on the number of parallel users and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

- **Transmission Encoding**

- **Automatic detection**

The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

- **Transmission Encoding**

- **Normal**

The Standard Encoding algorithm well suited for many parallel users and/or in a LAN environment.

- **Transmission Encoding**

- **Compressed**

The data stream between RAS-PutIn and the Remote Console window will be additionally compressed to save bandwidth. Choosing one of the rates between LAN (lowest) and GSM modem (highest) adjusts the compression rate. Typical applications generate traffic between 5 Kbytes/s (compression rate GSM modem) and 10 Kbytes/s (compression rate LAN). The compression encoding is well suited for a Modem or ISDN environment. However, since the compression takes processing time on RAS-PutIn itself, this encoding shouldn't be used when many parallel users want to access RAS-PutIn at the same time.

- **Start in Monitor Mode**

Sets the initial value for the monitor mode. By default the monitor mode is off. In case you switch it on, the Remote Console window will be started in a read only mode.

- **Exclusive Access**

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

- **Remote Console Type**

Specifies, which Remote Console Viewer to use.

- *Default Java-VM*

Uses the default Java Virtual Machine of your Browser. This may be the Microsoft JVM for the Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

- *Sun Microsystems Java Browser Plugin*

Instructs the Web browser of your administration system to use the JVM (Java Virtual Machine) of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with YES. The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM lays in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for this JVM versions and offers wider range of functionality when run in SUN's JVM. (Hint: If you are connected over a slow connection to the Internet you can also pre-install the JVM on your administration machine. The software is available on the CD that is delivered along with RAS-PutIn.)

- *ActiveX control*

This option instructs the Web browser to use the ActiveX-Control of the KVM Vision

Viewer, an application available separately. You have to install this program on your local system, please refer to the manual of the KVM vision viewer for further information. This option only works with Microsoft Internet Explorer on Win32 Systems.

- **Mouse hotkey**

Allows to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console (see Section 5.3.3 on page 27 for more information) or is used to leave the exclusive mouse mode (see below). The key codes are listed in Appendix C on page 71.

- **Button Keys**

Button Keys are meant for simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact, that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are ‘Control Alt Delete’ on Windows and DOS, what is always caught or ‘Control Backspace’ on Linux for terminating the X-Server. The syntax to define a new Button Key is as follows:

`[confirm] < keycode > [+ | - [*] < keycode >]*`

confirm requests confirmation by a dialog box before the key strokes will be sent.

keycode is the key to be sent. Multiple key codes can be concatenated with a + or a – sign. The + sign builds key combinations, all keys will be pressed until a – sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So the – sign builds single, separate keypresses and -releases. The * inserts a pause with a user-defineable duration(see Section 5.4.3 on page 37). For a list of key codes and aliases RAS-PutIn recognizes refer to Appendix C on page 71.

Pressing the Apply button finally changes the values permanently in RAS-PutIn.

5.3.6 Telnet Console

This options offers a Java applet for the Telnet protocol (5.10) to open a connection to RAS-PutIn. Its main use is the passthrough option for the serial port 1 (see also 5.5.5). The Telnet access has to be enabled in the security settings as well (see 5.5.10). Of course it is also possible to connect with a standard Telnet client. For details regarding the Telnet interface please refer to 5.6.

5.4 Server

5.4.1 Power Control

The appearance of the power control options depends on the power control option connected to RAS-PutIn and on the currently activated setting (see Section 5.5.5 on page 47 for an explanation). There are three options available:

- power control disabled
- internal power option
- external power option

Figure 5.9: Example of Remote Console settings

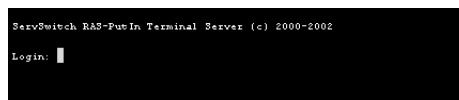


Figure 5.10: Telnet Console

Internal power option

For connecting the internal power option please refer to Section 3.3.3 on page 13. Once connected it has to be enabled using the serial settings (see Section 5.5.5 on page 47).

The Power Control panel enables access to the most important external buttons of your host system besides of the keyboard. These buttons are the reset and the ATX power button.

The power button is the representation of the ATX power button on your host system. It is used to switch on and off the power supply. The ATX power button knows two operation modes: pressing it shortly and pressing it for about 4 seconds. As shown in Figure 5.11 these two modes are supported separately. Table 5.2 explains the different effects.

Note: The prerequisite for the remote power/reset button to work is a correct installation of RAS-PutIn. The additional cabling as described in Section 3.3.3 on page 13 must be properly connected.

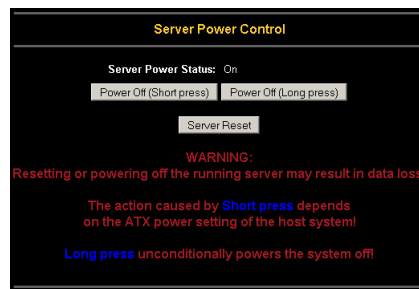


Figure 5.11: Internal Power Control

External power option

If an external power option is enabled the power control will look like shown in Figure 5.12.

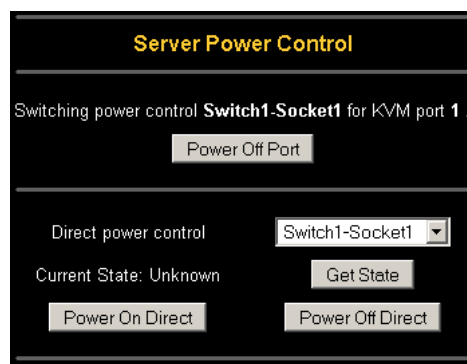


Figure 5.12: External Power Control

The upper half is used to switch the power for the KVM port currently active. Use the KVM settings (Section 5.4.3 on the next page) to assign a port of the external power control to a KVM port. If no assignment exists, the option is disabled.

The lower half offers controls for switching each port of the external power control directly. Select the appropriate port and decide whether to power it off or on.

The 'Get State' option is used to determine the current status of the selected port. It is executed once when the page gets loaded, if it is necessary to get the power state later just choose this option.

Power Control via IPMI When IPMI is enabled (Section 5.5.8), the power control section features the possibility to switch power or reset a system using IPMI (see Figure 5.13).

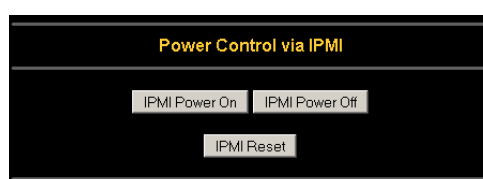


Figure 5.13: Power Control via IPMI

Table 5.2: Remote reset and power button effects

Button	Description
Reset	Pressing this button is similar to pressing the reset button directly on the remote system (see Figure 5.11). Be aware that pressing the reset button will result in unconditional and immediate cold start of the system. This might damage open files and the file system itself.
Power (short press)	<p>A short press on the ATX button is normally caught by the running operating system that tries to initiate a controlled shutdown.</p> <p>Usually this should always be the first action you try in case you would like to power off your system. Only in case this is not working you should try the long press button.</p> <p>Please note that after you have pressed this button the power state displayed in the administration panel won't immediately reflect the requested change. A controlled shut down of the system may take up to some minutes. You can observe the action caused by your button press using the Remote Console window or by reloading the Server Power Control panel.</p>
Power (long press)	<p>This will unconditionally power off the system. Even if you have submitted a short press before, this will shut down the power supply of the host system.</p> <p>The effect of the long button press can be immediately observed on the panel that is loaded into the browser because of the button press. The power state will be off.</p>

5.4.2 Keyboard/Mouse Settings

RAS-PutIn supports different keyboard and mouse models. The panel shown in Figure 5.14 on the next page is used to adjust those settings as well as some other ones. Their meaning is listed below:

- **Targeted KVM port**
Selects the KVM port the settings made below will be applied to. Choosing update will display the current values for this port and select it for alteration of its settings.
- **Keyboard Model**
Selects the keyboard model used on the remote host system.
- **Mouse Model**
Selects the mouse model that is used on the remote system. A wrongly selected mouse model may result in strange mouse effects.
- **Mouse Mode**
→ **Direct (1:n) mouse mode**
Use a direct translation of mouse movements between the local and the remote pointer. You may also set a fixed *Scaling* which determines the amount the remote mouse pointer moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on host are linear, means that there is no mouse acceleration involved.
- **Mouse Mode**

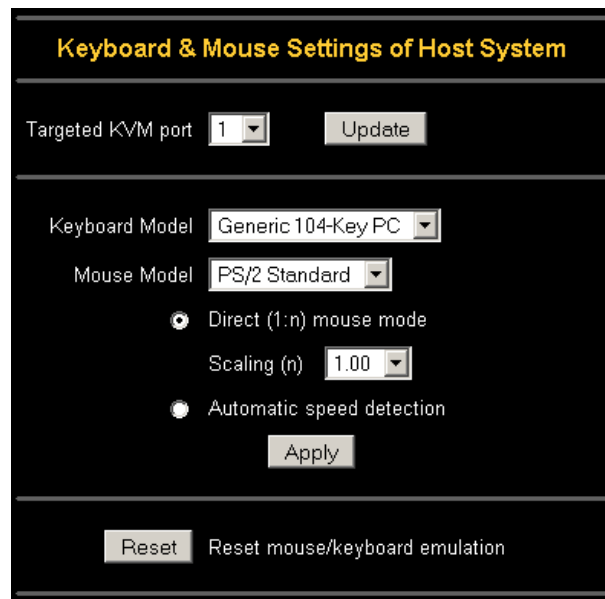


Figure 5.14: Keyboard/Mouse settings

→Automatic speed detection

Use this option if the mouse settings on host use an additional acceleration setting. RAS-PutIn tries to detect the acceleration and speed of the mouse during the mouse sync process.

- **Reset mouse/keyboard emulation**

This option will reset the RAS-PutIn keyboard and mouse emulation for the host system. Use it if the keyboard or mouse seems to react irrationally. Its just like pulling out the keyboard and mouse connectors and plugging them in again.

5.4.3 KVM Settings

The RAS-PutIn KVM settings (Figure 5.15 on the following page) allow to control a KVM switch located between RAS-PutIn and the hosts. Have a look at Section 3.1 on page 9 for a connection example.

It is possible to select the number of ports the connected KVM uses. Each port may get a name assigned. In order to provide KVM port switching through RAS-PutIn, key combinations have to be defined for the ports.

The syntax to define a new Hotkey is as follows:

$\langle \text{keycode} \rangle [+|-[*] \langle \text{keycode} \rangle]^*$
 For example: Ctrl-Ctrl-A-Enter
 or Ctrl+A-*1-Enter

Thereby *keycode* is the key to be sent. Multiple key codes can be concatenated with a + or a - sign. The + sign builds key combinations, all keys will be pressed until a - sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So the - sign builds single, separate keypresses and -releases. The * inserts a pause of user-defineable length, more than one * signs may be concatenated. The duration of a single pause

Nr	Name	Hotkey (Help)	Show in Console
1	Server 1	ctrl-ctrl-1-enter	<input checked="" type="checkbox"/>
2	Server 2		<input type="checkbox"/>
3	Firewall		<input type="checkbox"/>
4	Printserver		<input type="checkbox"/>

Figure 5.15: KVM Settings

is set in milli seconds using the appropriate option on the KVM settings page. See Appendix C on page 71 for a list of key codes that can be used as hotkeys.

Note: The settings will be saved only after pressing ‘Apply’.

If the settings are correct, the KVM port can be switched using the option ‘Active port’ on top of this page or with the KVM switching matrix on the RAS-PutIn homepage (see Section 5.2.2 on page 21). RAS-PutIn uses separate mouse synchronization settings (see section 5.3.3 on page 27) and video-settings (see Section 5.3.4 on page 28) for each port.

Note:

It is still possible to apply KVM key combinations through the Remote Console for switching KVM port, however, in this case video and mouse synchronization settings will be shared among the ports and may unintentionally be changed for one of those ports.

External Power Switch Option If an external power option is enabled it is additionally possible to assign a port of this control for power switching to each KVM port (see Section 5.4.1 on page 36).

5.5 Administration

5.5.1 User/Group Management

The user and group management of RAS-PutIn is based on configurable users and groups. Each user or group may have different permissions.

Upon delivery, each RAS-PutIn is pre-configured with a supervisor user called ‘super’ having the password rasputin. Make sure to change the super user password immediately after you have installed and firstly accessed your RAS-PutIn.

Figure 5.16 shows the User/Group Management panel of the RAS-PutIn front-end. Its use will be described in the following text.

The image shows a web interface with two main sections: 'User Management' and 'Group Management'. The 'User Management' section includes a dropdown for 'Existing users' with a 'Lookup User' button, and input fields for 'New user name', 'Full user name', 'Password' (with a strength indicator 'AAAA'), 'Confirm Password', 'Email address', and 'Mobile number'. Below these is a 'Group membership' section with two lists: 'Member of' and 'Not Member of supergroup', connected by left and right arrow buttons. At the bottom of this section are buttons for 'Create User', 'Modify User', 'Copy User', and 'Delete User'. The 'Group Management' section has a dropdown for 'Existing groups' and an input field for 'New group name', with buttons for 'Create Group', 'Modify Group', 'Copy Group', and 'Delete Group'.

Figure 5.16: User/Group Management

- **Existing user**
Select an existing user for modification or deletion. Once a user has been selected, click the lookup button to see the complete user information.
- **New user name**
In order to create a new user, enter a new login name in this field. The new name must not yet exist as user or group. In case it does, an error message will be displayed on top of the panel.
- **Full user name**
This name is the full name belonging to the login name.
- **Password**
The password for the login name. It must be at least four characters long.
- **Confirm password**
Confirmation of the password above.
- **Email address**
This is optional.
- **Mobile number**
This information may be optionally provided.
- **Group membership**
Each user can be a member of one or more groups.
- **Existing groups**

Selects an existing group for copying, modification or deletion.

- **New group name**

In order to create a new group, enter a new and unused group name.

The user management of RAS-PutIn allows many different users. The following sections will describe how to add, change and delete users.

5.5.1.1 Add User

Fill out the fields ‘New user name’, ‘Full user name’, ‘Password’ and ‘Confirm password’ as shown in Figure 5.16 on the preceding page. Optionally select the groups the new user should become a member of. Click the ‘Create user’ button.

5.5.1.2 Delete User

Select a user in the ‘Existing user’ control. Click the ‘Lookup’ button. The complete user information will be shown. Click the ‘Delete user’ button.

Hint:

The pre-configured supervisor user ‘super’ can’t be deleted. This user can be renamed only.

5.5.1.3 Modify User

Select a user in the ‘Existing user’ control. Click the lookup button to get all the user’s information. All fields can be modified as required. The old password is not displayed, but can be modified. If all changes are done click the ‘Modify user’ button.

5.5.1.4 Copy User

Select a user in the ‘Existing user’ control. Enter a new user name in the field ‘New user name’. Click the ‘Copy User’ button. This will create a new user with the given name. All properties of the selected user will be copied to the new one, except user specific permissions.

5.5.1.5 Add Group

Type the name of the new group into the field ‘New group name’ and click the ‘Create group’ button.

5.5.1.6 Delete Group

Select a group in the ‘Existing group’ control. Click the ‘Delete group’ button.

5.5.1.7 Modify Group

To modify an existing group select the group in the ‘Existing group’ control. The group’s name field can be modified. Finally click the ‘Modify group’ button.

5.5.1.8 Copy Group

Select a group in the ‘Existing group’ control and type the name of the new group into the field ‘New group name’. Click the ‘Copy Group’ button. This will create a new group and copy all properties and permissions of the selected group to the newly created group.

5.5.2 User/Group Permissions

A set of permissions is assigned to each user or group. Those rights are used to authorize access to certain RAS-PutIn functionality for a particular user. By default the user ‘super’ has all permissions. His permissions cannot be shrunk. A newly created user or group has no permissions. A user will inherit the permissions of all groups he belongs to.

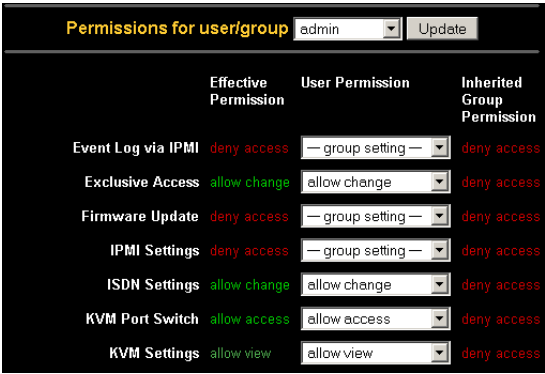


Figure 5.17: User/Group Permissions panel

The User/Group Permissions panel as shown in Figure 5.17 allows you to change the permissions of a certain user or group. The right of one user for changing another user’s or group’s access rights is determined by the parent/child relationship between them. When one user is creating another user, he will implicitly become the parent of that new user and hence has the right to change his permissions. More general, a certain user has the right to change another user’s or group’s permissions in case he stands higher in the ancestry than the other one. The ‘super’ user stands at the top (or the root) of the ancestry, hence has the right to change everybody’s permissions.

Additionally, there is the restriction that a user can never give more permission to others than those he has. For example, if a user has no permission to change the network settings he won’t be able to grant this right to somebody else. However, a user has always the right to reduce the set of permissions of his descendants.

In order to change the permissions of a user/group you have to select the user/group first. This is done using the selection list at the top of the User/Group Permissions panel (see Figure 5.17 on the preceding page). The selection list will show only users and groups for which you have the right to change their permissions. Next, clicking the ‘Update’ button will show the permission list of that user. Every right in the list has a permission value, which is explained in Table 5.3.

The displayed columns differ, depending on the user/group selected and the one logged in:

Effective Permission	The final permission which decides if a user may access a specific RAS-PutIn function or not.
----------------------	---

User Permission	Permission for the currently selected user/group. If the user selected equals to the one logged in it is only possible to view the value, otherwise a select box appears to change it.
Inherited Group Permission	Permission value inherited from the groups a user belongs to. This column is not available while a group is selected.

Table 5.3: RAS-PutIn user and group permissions

Field	Description
deny access	The user cannot use this function.
allow view	The user can view the entry.
deny change	The user cannot change the entry's settings.
allow change	The user can change the entry settings.
allow access	The user can use this function.
group setting	No permission, use the one inherited from the group(s) the user belongs to. Default is to deny access.

5.5.3 Network Settings

The Network Settings panel as shown in Figure 5.18 on the facing page allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

Note:

The initial IP configuration is usually done directly at the host system using the special procedure described in Section 4.1 on page 15. However you can also connect to the RAS-PutIn using its pre-configured IP settings.

Attention:

Changing the network settings of RAS-PutIn might result in losing connection to it. In case you change the settings remotely make sure all the values are correct and you still have an option to access the RAS-PutIn.

- **IP auto configuration**

With this option you can control if RAS-PutIn should fetch it's network settings from a DHCP or BOOTP server. For DHCP you have to enter *dhcp* and for BOOTP supply *bootp* accordingly. If you specify *none* then IP autoconfiguration is disabled.

- **IP auto configuration timeout**

Time within a DHCP/BOOTP server is expected to respond to the RAS-PutIn DHCP/BOOTP client request. If there is no response, the last known IP settings will be used to configure RAS-PutIn.

- **IP address**

IP address in the usual dot notation.

- **Subnet mask**

The net mask of the local network.

- **Gateway IP address**

In case the RAS-PutIn should be accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

Figure 5.18: RAS-PutIn network settings

- **Primary DNS Server IP address**
IP address of the primary Domain Name Server in dot notation. This option may be left empty, however RAS-PutIn won't be able to perform name resolution.
- **Secondary DNS Server IP address**
IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server can't be contacted.
- **Primary Time Server**
IP address of the primary NTP (Network Time Protocol) compliant timeserver in dot notation. RAS-PutIn will synchronize its own absolute time with the timeserver's one. This is important for writing log entries and for the Dynamic DNS Service.
- **Secondary Time Server**
IP address of the secondary NTP compliant timeserver in dot notation. It will be used in case the Primary Time Server can't be contacted.
- **Remote Console & HTTPS port**
Port number at which RAS-PutIn's Remote Console server and HTTPS server are listening. If left empty the default value will be used.
- **HTTP port**
Port number at which RAS-PutIn's HTTP server is listening. If left empty the default value will be used.
- **Telnet port**
Port number at which RAS-PutIn's Telnet server is listening. If left empty the default value will be used.
- **Bandwidth limitation**
The maximum network traffic generated through the RAS-PutIn ethernet device. Unit is Kbit/s.
- **Disable Peppercon-EMX Support**
With this option you may exclude this RAS-PutIn from management by a Peppercon-EMX.

5.5.3.1 Dynamic DNS

Blackbox provides a Dynamic DNS service that can be used in the following scenario (see Figure 5.19):

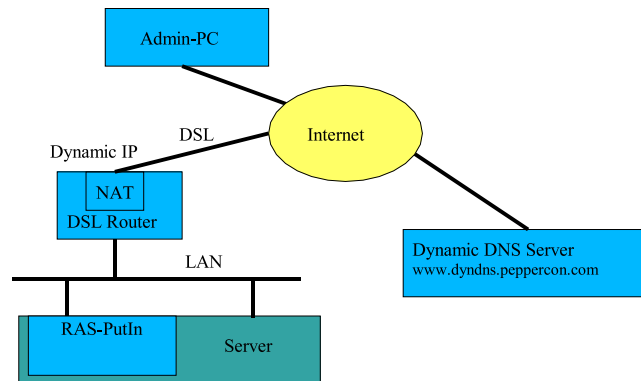


Figure 5.19: Dynamic DNS Scenario

RAS-PutIn is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator doesn't know the IP address assigned by the provider, RAS-PutIn connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to his card.

The administrator has to register a RAS-PutIn that is supposed to take part in the service with the Dynamic DNS Server. He will get an approved nickname and password in return to the registration process. This account information is needed in order to determine the IP address of the registered RAS-PutIn.

Figure 5.20: Dynamic DNS configuration panel

You have to perform the following steps in order to enable Dynamic DNS:

1. Make sure the LAN interface of RAS-PutIn is properly configured.
2. Enter the Dynamic DNS Settings configuration dialog as shown in Figure 5.20 on the next page (Menu → Network Settings → Dynamic DNS Settings)
3. Enable Dynamic DNS and change the settings according to your needs (see below).
 - **Enable Dynamic DNS**
This enables the Dynamic DNS service. This requires a configured DNS server IP address.
 - **Dynamic DNS server**
Here you enter the server name where RAS-PutIn registers itself in regular intervals. If

left blank the default will be used.

- **Nickname**

You have registered this nickname during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname!

- **Check time**

RAS-PutIn card registers itself in the Dynamic DNS server at this time.

- **Check interval**

This is the interval for reporting again to the Dynamic DNS server by RAS-PutIn.

Note:

RAS-PutIn has its own independent real time clock. Make sure the time setting of RAS-PutIn is correct. This can be achieved by configuring a timeserver (see Figure 5.18 on page 43)

Note:

RAS-PutIn registers itself to the Dynamic DNS server slightly different from the time configured. To reduce load peaks on the server we add a random time (0-10 min) to the absolute time value.

5.5.4 SNMP Settings

The following information is available via SNMP:

- Serial number
- Firmware version
- MAC address / IP address / Netmask / Gateway of LAN interface
- Configured users
- Currently active users with login time (login time is only valid if time is synchronized on RAS-PutIn)
- Server's power state
- The following actions can be initiated via SNMP:
 - Reset server
 - Power on/off server
 - Reset RAS-PutIn

The following events are reported by RAS-PutIn via SNMP:

- Login trial at RAS-PutIn failed.
- Login trial at RAS-PutIn succeeded.
- Denying access to a particular action.
- Server was reset.
- Server was powered on/off.

The SNMP settings panel as shown in Figure 5.21, described below, allows you to change SNMP related parameters.

The figure shows a web-based configuration interface for SNMP settings. It is organized into three main sections, each with a yellow header:

- Agent:** Contains a checkbox labeled 'Enable SNMP Agent'. Below it are four text input fields: 'Read Community', 'Write Community', 'System Location', and 'System Contact'.
- Traps:** Contains three checkboxes: 'Enable SNMP Authentication Traps', 'Enable ServSwitch RAS-PutIn Authentication Traps', and 'Enable Host Traps'.
- Trap Destinations:** Contains a table with two columns, 'IP address' and 'Community'. The first row is labeled 'Entry 1'. Below the table is a button labeled 'More entries'.

Figure 5.21: SNMP settings

- **Enable SNMP Agent**

If this option is checked, RAS-PutIn will answer to SNMP requests. Hint: If a community is left blank, you cannot perform the according request. E.g. if you want to disable the possibility to reset RAS-PutIn via SNMP then don't set a write community.

- **Read Community**

This is the SNMP community, which allows you to retrieve information via SNMP.

- **Write Community**

This community allows you to set options and to reset RAS-PutIn or the host via SNMP, i.e. all that effects the host or RAS-PutIn.

- **System Location**

Enter a description of the physical location of the host. The description will be used in reply to the SNMP request "sysLocation.0".

- **System Contact**

Enter a contact person for the host. The value will be used in reply to the SNMP request "sysContact.0".

- **Enable SNMP Authentication Traps**

If this option is checked, an SNMP trap will be sent in case somebody has tried to access RAS-PutIn via SNMP using a wrong SNMP community.

- **Enable RAS-PutIn Authentication Traps**

If this options is checked, an SNMP trap will be sent in case somebody has tried to login via

the Web front-end. Both successful and failed logins trials will be indicated. Furthermore, there will be notification about other security violations like trying to perform an action via Web front-end for which a user has no permission.

- **Enable Host Traps**

If this option is checked, RAS-PutIn will send SNMP traps whenever the host is reset, powered down or powered up.

- **Trap destinations**

Here you can enter the IP addresses, to which the traps will be sent. For every IP address, you have to set an according community. This is necessary so that your management client can identify the SNMP traps.

The RAS-PutIn SNMP MIB This link allows you to download the RAS-PutIn SNMP MIB file. This file may be necessary for an SNMP client to communicate with RAS-PutIn.

5.5.5 Serial Settings

The RAS-PutIn Serial Settings (Figure 5.22 on the following page) allow you to specify, what devices are connected to the two serial ports and how to use them.

Serial Port 1 This port may be used for different purposes. All possible options are listed and described below.

- **Configuration login**

Don't use the serial port for any special function, use it only for the initial configuration (see Section 4.1 on page 15).

- **Modem**

Allows to access RAS-PutIn via modem, see Section 5.5.6 on page 49 for details.

- **IPMI over Serial**

Enables the possibility to use this serial port for IPMI 1.5 over serial, check Section 5.5.8 on page 52 for more information.

- **Passthrough**

Using this option, it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via telnet. Select the appropriate options for the serial port and use the Telnet Console (see Section 5.3.6 on page 33) or a standard telnet client to connect to RAS-PutIn. For more information about the telnet interface have a look at Section 5.6 on page 62.

Serial Port 2 This serial port provides the power control options for RAS-PutIn (see also Section 5.4.1 on page 34). Choose a suitable setting and fill in additional required options. By the date of printing this manual RAS-PutIn supports the following options

Internal Power Option	The optionally available internal power bracket allows to access the ATX power and reset functions of a single system connected to RAS-PutIn. See Section 3.3.3 on page 13 for details. For this power option it is possible to change the duration of each button press. Choosing the link besides the option will lead to the form in Figure 5.23 on the
-----------------------	--

Serial Port 1

☒ Configuration login

☒ Modem

Serial line speed: 115200 bits/s

Modem init string: "ATZHD OK ATLDMD&K3X1 OK" is used if empty.

Client IP address: 192.168.3.1

☐ IPMI over serial

☐ Passthrough access to serial port via Telnet

Serial Line speed: 115200 bits/s

Data bits: 8

Parity: none

Stop bits: 1

Handshake: None

Serial Port 2

☒ Disabled

☐ Internal power option [Change button press durations](#)

☒ External power option

☒ SPC 800/1600

Username:

Password:

☐ IPM 220-L (Inline Power Modul)

☐ ePowerSwitch

☒ ePowerSwitch-M/S

Figure 5.22: Serial Settings

facing page. It features an entry field for the durations of a reset, a short and a long power press.

SPC 800/1600

Using the Avocent™SPC³ it is possible to switch power for more than one system connected to RAS-PutIn through a KVM switch. To use this device you have to enter an username and a password which must exist on the SPC and have the privileges to switch power for each port.

Intelligent Power Module

This is an optionally available external module to switch power of a single system by putting it in the power supply line of the controlled system.

ePowerSwitch

The ePowerSwitch is a 4-port power socket. Each single port can be switched using an integrated web browser or the serial port. RAS-PutIn supports the serial connection.

³Avocent is a registered trademark of Acovent Corp. Huntsville

ePowerSwitch-M/S The ePowerSwitch-M/S is a cascade of up to 4 power sockets with 8 ports. RAS-PutIn has to be connected to the first socket of the cascade via a serial connection.

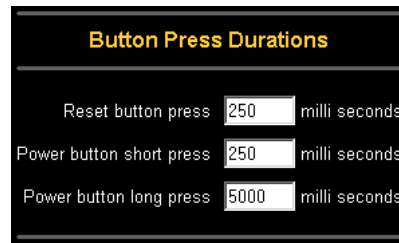


Figure 5.23: Internal Power Option Settings

5.5.6 Modem Settings

RAS-PutIn offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to RAS-PutIn's serial interface.

Logically, connecting to RAS-PutIn using a telephone line means nothing else than building up a dedicated point to point connection from your console computer to the RAS-PutIn. With other words, RAS-PutIn acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to RAS-PutIn, make sure to configure your console computer accordingly. For instance on Windows based operating systems you can configure a dial-up network connection, which defaults to the right settings like PPP.

The modem settings are part of serial settings panel (Figure 5.22 on the preceding page).

- **Enable modem on RS 232**

Enable or disable the modem on the serial interface adapter of RAS-PutIn. In case it is enabled, RAS-PutIn tries to initialize the modem using an initial string of AT commands and waits for incoming connections.

- **Serial line speed**

The speed RAS-PutIn is communicating with the modem. Most of all modems available today will support the default value of 115200 bps. In case you are using an old modem and discovering problems try to lower this speed.

- **Modem Init String**

The initialization string used by RAS-PutIn to initialize the modem. The default value will work with all modern standard modems directly connected to a telephone line. In case you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by giving a new string. Refer to the modem's manual about the AT command syntax.

- **Client IP address**

This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure, it is not interfering with the IP settings of RAS-PutIn and your console computer. The default value will work in most cases.

5.5.7 ISDN Settings

In addition to the standard interfaces, RAS-PutIn offers remote access using an ISDN connection⁴.

Logically, connecting to RAS-PutIn using an ISDN line means nothing else than building up a dedicated point to point connection from your console computer to RAS-PutIn. With other words, RAS-PutIn acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to RAS-PutIn, make sure to configure your console computer accordingly.

The ISDN settings panel (see Figure 5.24 on the facing page) allows you to configure RAS-PutIn for an ISDN connection. The according ISDN options are described below.

- **Enable ISDN**
Enables or disables the ISDN adapter.
- **MSN**
This Multiple Subscriber Number is assigned to RAS-PutIn. Hint: The RAS-PutIn ISDN function does not work with empty MSN.
- **Layer-2 protocol**
The Layer-2 Protocol (the Data Link Layer) of the ISO 7-layered architecture. It is responsible for the error-free movement of data between network nodes. You can choose between the High-level Data Link Control (HDLC) and X.75. You can leave this option untouched in case you use a standard network connection as built in Windows or Linux.
- **Enable hang-up timer for incoming calls**
If you want RAS-PutIn to hang up an incoming connection, you have to check this box. The time out value is configured using the next option.
- **Hang-up timeout**
The hang-up time out measured in seconds. Normally it is valid for outgoing connections only. That means, in case RAS-PutIn is configured for callback. In case the 'Enable hang-up timer for incoming calls' option is checked, the time out will apply for incoming calls also.
- **IP address range**
Addresses from this range will be assigned to RAS-PutIn and the console computer during establishing an ISDN connection. The first address will be used for RAS-PutIn itself. The range must enclose 3 addresses at least.
- **Enable callback**
This enables the callback mechanism. If you have callback entries configured (see below) RAS-PutIn will reject any call from the configured number(s) and make a call to a number, which can be configured too.
- **Force callback**
Only callback connections are enabled if you enable this option. That means nobody can dial in without callback. This option has effect only if you have callbacks enabled.
- **Calling #**
This is the calling number - the client that tries to dial into RAS-PutIn.

⁴ISDN is available for EMEA versions of RAS-PutIn only

- **Called #**

If you want to call the caller back, you have to enter his number here.

- **User / Password**

If RAS-PutIn calls back these are the user name and the corresponding password for authentication on the console computer.

- **Call back after [x] seconds**

The entry is marked as a callback entry in case this checkbox is checked. Additionally, the delay, after which the callback connection will be established, can be configured. Callback entries are only effective when the callback mechanism is enabled.

General ISDN Settings

☐ Enable ISDN

MSN

Layer-2 protocol

☐ Enable hangup timer for incoming calls

Hangup timeout seconds

IP address range to

ISDN Dialin and Callback Settings

☐ Enable callback ☐ Force callback

	Calling #	Called # (callback only)	User (callback only)	Password (callback only)
Entry 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

☐ call back after seconds.

NOTE: If you have none or only callback entries configured anyone may dialin unless callbacks are enabled and forced.

Figure 5.24: RAS-PutIn ISDN settings panel

In the following, we will present some example use cases for a proper ISDN configuration.

5.5.7.1 I want to allow non-callback dial in for everyone.

To achieve this you have to switch off the "Force callback" option and you should have no callback entries configured.

5.5.7.2 I want to allow non-callback dial in for selected people.

First, make sure "Force callback" is switched off. Second, you have to make an entry with the calling number for every allowed client. The other fields should be left empty. There must be at least one non-callback entry or anyone can dial in!

5.5.7.3 I want to allow non-callback dial in for everyone except some people that should be called back.

Make sure you have callback enabled and "Force callback" is switched off. Now configure an entry for every number that should be called back. Don't forget to mark the entries as callback entries! The list should contain callback entries only.

5.5.7.4 I want to allow non-callback dial in for selected people except some people that should be called back.

Make sure you have callback enabled and "Force callback" is switched off. Then you have to make an entry for every allowed client. For callback entries, all fields have to be specified. There must be at least one non-callback entry or anyone can dial in!

5.5.7.5 I want to allow callback connections only.

Make sure you have callback enabled and "Force callback" is switched on. You have to make an entry for every allowed client. Don't forget to mark the entries as callback entries!

5.5.8 IPMI Settings

5.5.8.1 Generals

By using the RAS-PutIn IPMI (Intelligent Platform Management Interface) facilities, you have an additional way to power on or off the system or to perform a hard reset. Furthermore, it provides the possibility to show an event log of the host system and the status of some system sensors (i.e. temperature). If your host system supports IPMI, you can access it by one of the following ways:

- IPMI over Serial (IPMI V1.5 is required)
- IPMI over LAN (IPMI V1.5 is required)

5.5.8.2 IPMI Settings

Figure 5.25 shows the RAS-PutIn IPMI settings panel. Its options will be explained below.

- **IPMI disabled**
Disables IPMI on RAS-PutIn. This means that Status via IPMI and Event Log via IPMI are not available and the power on/off and reset functions don't use IPMI rather than the ATX and the reset cable connected from RAS-PutIn to the motherboard.
- **BMC address**
The hexadecimal Baseboard Management Controller address, which is needed for all communication types to the IPMI-interface. Usually you can find this address in the BIOS of the host system. The default and common value for this address is 20.
- **IPMI over IPMB**
This connection type uses an IPMB cable connected from the 1x5pin IPMB connector on the RAS-PutIn card to the 3/4pin IPMB/I2C connector on the motherboard. IPMI over

Figure 5.25: IPMI settings panel

IPMB doesn't need any passwords. This access mode allows only power on/off and reset function. Status and Event Log via IPMI are disabled.

- **IPMI over Serial**

If your host system supports IPMI V1.5 and has an Intel EMP (Emergency Management Port, usually COM2) connector, you can connect IPMI through serial port 1 on RAS-PutIn. There are some additional points to note:

- The EMP port must be set to 'Always enable' and the 'Restricted Mode' must be switched off.
- The BMC should accept a 'null username' and a 'non-null password' account as login.
- Passwords are 4 - 16 characters long.
- A null modem cable is used for connection

- **IPMI over LAN**

You can connect the IPMI over a LAN connection too. The prerequisite for this access type is a host system with IPMI V1.5 and a network adapter with a sideband connection to the BMC (mostly on board). In the IPMI Settings, you must enter the IP-address of this host system and the correct password for the LAN connection. You can also access other IPMI systems when you enter their IP address.

5.5.8.3 Power Control

If IPMI is enabled, these functions are performed over IPMI requests. These requests may take a few seconds.

If IPMI is disabled, the power control functions (power on, power off, reset) are performed over the internal or external power control options.

5.5.8.4 Event Log via IPMI

The Event Log via IPMI accesses the SEL (System Event Log) repository and reads every entry sequentially. The first time you use this function after starting RAS-PutIn the complete

repository has to be read, what may take 1 or 2 minutes.

Figure 5.26: IPMI Event Log

When all entries have been read, RAS-PutIn displays the entries with their time, sensor and description in accordance with the filter settings. You have the choice between several pre-settings (i.e. last day, last week) or an exact declaration of the start and the end date.

Once you changed the filter settings, click on ‘Update’ in order to update the shown entries (see Figure 5.26). If the checkbox ‘Get sensor names’ is checked all sensor IDs will be shown with their respective names.

The time that is shown in the log entries is the SEL time, which means that this time is independent to the system time. The actual SEL time is shown at the top of the log table.

With the button ‘Clear Event Log’ you can delete all entries in the SEL repository.

5.5.8.5 Status via IPMI

Fan Status						
Name	Status	Value	Min (crit.)	Min	Max	Max (crit.)
Baseboard Fan 1	OK	4410	480	630		
Pwr Cage Fan 1	OK	10266	0	0		
Pwr Cage Fan 2	OK	10010	0	0		
Temperature Status						
Name	Status	Value	Min (crit.)	Min	Max	Max (crit.)
Baseboard Temp	OK	23.0	0.0	3.0	47.0	50.0
Frontpanel Temp	OK	22.0	0.0	3.0	45.0	48.0
Voltages						
Name	Status	Value	Min (crit.)	Min	Max	Max (crit.)
Baseboard 1.5V	OK	1.51	1.27	1.35	1.65	1.73
Baseboard 2.5V	OK	2.53	2.14	2.25	2.74	2.88
Baseboard 3.3V	OK	3.35	2.80	2.98	3.63	3.79

Figure 5.27: Example of IPMI State panel

The Status via IPMI function shows the current values and the min/max-thresholds of all fans, temperatures and voltages existing in the host system. An example of such an IPMI panel is shown in Figure 5.27 on the next page. You can change the thresholds by editing the according values and pressing ‘Apply’.

The first time you call this page, it may take up to two minutes until the sensor data will be shown.

Note:

If IPMI is disabled, Status via IPMI and System Log via IPMI are not available (the corresponding menu options are not visible).

5.5.9 LDAP Settings

5.5.9.1 Generals

With RAS-PutIn you have the possibility to keep authentication information in a central LDAP directory. To use this feature you need to configure an LDAP server that contains these information. The settings are explained in the following.

5.5.9.2 LDAP Settings

Figure 5.28 shows the RAS-PutIn LDAP settings panel. Its options will be explained below.

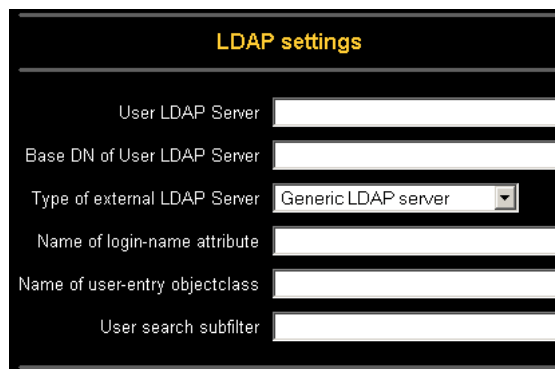


Figure 5.28: LDAP settings panel

- **User LDAP Server**

Here you enter the name or IP address of the LDAP server containing all the user entries. If you choose a name instead of an IP address you need to configure a DNS server in the network settings.

- **Base DN of User LDAP Server**

Here you specify the distinguished name (DN) where the directory tree starts in the user LDAP server.

- **Type of external LDAP Server**

With this option you set the type of the external LDAP server. This is necessary since some server types require special handling. Additionally the default values for the LDAP schema are set appropriately. You can choose between *Generic LDAP Server*, *Novell Directory Service* and *Microsoft Active Directory*. If you have neither Novell Directory Service nor Microsoft Active Directory then choose *Generic LDAP Server* and edit the LDAP schema used (see below).

- **Name of login-name attribute**

This is the name of the attribute containing the unique login name of a user. To use the default leave this field empty. The default depends on the selected LDAP server type.

- **Name of user-entry objectclass**

This is the objectclass that identifies a user in the LDAP directory. To use the default leave this field empty. The default depends on the selected LDAP server type.

- **User search subfilter**

Here you can refine the search for users that should be known to the RAS-PutIn.

- **Active Directory Domain**

This option represents the active directory domain that is configured in the Microsoft Active Directory server. This option is only valid if you have chosen *Microsoft Active Directory* as the LDAP server type.

5.5.10 Security Settings

Figure 5.29 on the next page shows the panel for security related SSL, Telnet and IP address settings. Each of those categories will be explained in the following subsections.

The screenshot shows a web interface for security settings. It is divided into three main sections: SSL Settings, TELNET Settings, and IP Access Control.

SSL Settings: Includes a checkbox for "Force HTTPS", a "KVM Encryption" section with radio buttons for "Off", "Try", and "Force", and a link: "Follow this link if you want to create your own SSL certificate."

TELNET Settings: Includes a checkbox for "Enable TELNET access".

IP Access Control: Includes a checkbox for "Enable IP Access Control", a "Default policy" dropdown menu set to "ACCEPT", and a table for defining rules.

Rule #	IP/Mask	Policy
<input type="text"/>	<input type="text"/>	ACCEPT

Below the table are four buttons: "Append", "Insert", "Replace", and "Delete".

Figure 5.29: Security settings

5.5.10.1 SSL Settings

Table 5.4 explains the possible adjustments related to the usage of SSL.

Table 5.4: Security parameters

Parameter	Description
Force HTTPS	If this option is enabled access to the Web front-end is only possible using an HTTPS connection. RAS-PutIn won't listen on the HTTP port for incoming connections. In case you want to create your own SSL certificate that is used to identify this RAS-PutIn refer to Section 5.5.11 on page 59.
KVM encryption	This option controls the encryption of the RFB protocol, the protocol used by the Remote Console to transmit the screen data to the administrator machine and keyboard and mouse data back to the host. If set to 'Off' no encryption will be used. If set to 'Try' the applet tries to make an encrypted connection. In case connection establishment fails for any reason an unencrypted connection will be used. If set to 'Force' the applet tries to make an encrypted connection. An error will be reported in case connection establishment fails.

5.5.10.2 Telnet Settings

Table 5.5 explains the settings related to Telnet access.

Table 5.5: Telnet security settings

Parameter	Description
Enable Telnet access	If this option is enabled, access over Telnet client is possible. For higher security we recommend to disable Telnet access.

5.5.10.3 IP Access Control

This section explains the settings related to IP access control. It is used to limit access to a distinguished number of clients only. These clients will be identified by their IP address, from which they are trying to build up a connection. Refer also to Figure 5.29 on the page before.

Note:

The IP access control settings apply to the LAN interface only!

- **Enable IP Access Control**

Enables access control based on IP source addresses.

- **Default policy**

This option controls what to do with arriving IP packets that don't match any of the configured rules. They can be accepted or dropped.

ATTENTION:

If you set this to DROP and you have no ACCEPT rules configured, access to the Web front-end over LAN is actually disabled! To enable access again you can change the security settings via modem or ISDN dial in or by temporarily disabling IP access control with the initial configuration procedure (see Section 4.1 on page 15).

- **Rule Number**

This should contain the number of a rule for which the following commands will apply. This field will be ignored, in case of appending a new rule.

- **IP/Mask**

Specifies the IP address or IP address range for which the rule applies.

Examples (the number concatenated to an IP address with a ‘/’ is the number of valid bits that will be used of the given IP address):

192.168.1.22/32 matches the IP Address 192.168.1.22

192.168.1.0/24 matches all IP packets with source addresses from 192.168.1.0 to 192.168.1.255

0.0.0.0/0 matches any IP packet

- **Policy**

The policy determines what to do with matching packets. They can be accepted or dropped.

NOTE: The order of the rules is important. The rules are checked in ascending order until a rule matches. All the rules below the matching one will be ignored. The default policy applies if no match has been found.

- **Appending a rule**

Enter the IP/Mask and set the policy. Finally, press ‘Append’.

- **Inserting a rule**

Enter the rule number, the IP/Mask and set the policy. Finally, press ‘Insert’.

- **Replacing a rule**

Enter the rule number, the IP/Mask and set the policy. Finally, press ‘Replace’.

- **Deleting a rule**

Enter the rule number and press ‘Delete’.

5.5.11 SSL Certificate Management

RAS-PutIn uses the SSL⁵ protocol for any encrypted network traffic between itself and a connected client. During connection establishment, RAS-PutIn has to expose its identity to a client using a cryptographic certificate. Upon delivery, this certificate is the same for all RAS-PutIns ever produced and certainly won’t match the network configurations that will be applied to the card by its user. The certificate’s underlying secrete (private) key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all).

- **Common name**

This is the network name of RAS-PutIn once it is installed in the user’s network (usually the fully qualified domain name). It is identical to the name that is used to access the card with a Web browser (without the ‘http://’ prefix). In case the name given here and the actual network name differ, the browser will pop up a security warning when the card is accessed over HTTPS.

⁵SSL — Secure Socket Layer

- **Organizational unit**
This field is used for specifying to which department within an organization RAS-PutIn belongs.
- **Organization**
The name of the organization to which RAS-PutIn belongs.
- **Locality/City**
The city where the organization is located.
- **State/Province**
The state or province where the organization is located.
- **Country**
The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany or US for the USA.
- **Challenge Password**
Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is 4 characters.
- **Confirm Challenge Password**
Confirmation of the Challenge Password
- **Email**
The email address of a security contact person that is responsible for RAS-PutIn.
- **Key length**
This is the length of the generated key in bits. 1024 Bits are supposed be sufficient for most cases. Larger keys may result in slower response time of RAS-PutIn during connection establishment.

However, it is possible to generate and install a new certificate that is unique for a particular card. In order to do that, RAS-PutIn is able to generate a new cryptographic key and the associated so called Certificate Signing Request that needs to be certified by a so called certification authority (CA). A certification authority verifies that you are who you claim you are and signs and issues a SSL certificate to you.

The following steps are necessary to create and install a RAS-PutIn SSL certificate:

1. Create a SSL Certificate Signing Request using the panel shown in Figure 5.30 (Security Settings → SSL Settings → Create your own SSL certificate). You need to fill out a number of fields that are explained above. Once this is done, click ‘Create CSR’ which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the ‘Download CSR’ button (see Figure 5.31 on the facing page).
2. Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).
3. Upload the certificate to RAS-PutIn using the ‘Upload’ panel as shown in Figure 5.31 on the next page.

After completing these three steps, RAS-PutIn has its own certificate that is used for identifying the card to its clients.



SSL Certificate Signing Request (CSR)

Common name

Organizational unit

Organization

Locality/City

State/Province

Country (ISO code)

Email

Challenge password

Confirm Challenge password

Key length (bits)

Create CSR

Figure 5.30: SSL Certificate Request

Important Note:

If you destroy the CSR on RAS-PutIn there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps.

5.5.12 Maintenance

RAS-PutIn Board Summary This section contains a summary with various information about this RAS-PutIn and its current firmware and allows you to reset RAS-PutIn. Have a look at Figure 5.34 on page 63 for an example.

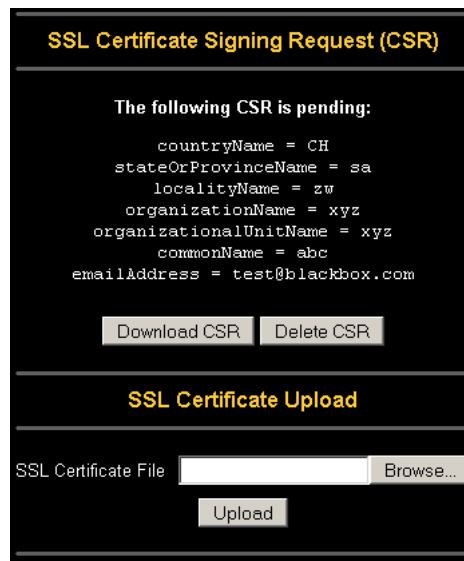
Data file for support This link allows you to download the RAS-PutIn data file with support information. This is an XML file with certain customized support information like the serial number etc. You may send this information along together with a support request. It will help us troubleshooting your problem.

Reset RAS-PutIn This part allows you to reset RAS-PutIn. This function is mainly needed to activate a newly updated firmware. A reset will close all current connections to the administration console or to the Remote Console. The whole process will take about half a minute.

5.5.12.1 Update Firmware

RAS-PutIn is a complete standalone computer. The software it runs is called the firmware. The firmware of RAS-PutIn can be updated remotely in order to install new functionality or special features.

A new firmware update is a binary file which will be sent to you by email or which you can download from the Blackbox Web site. If the firmware file is compressed (file suffix .zip) then you must unzip it before you can proceed. Under the Windows operating system you may



SSL Certificate Signing Request (CSR)

The following CSR is pending:

```
countryName = CH
stateOrProvinceName = sa
localityName = zw
organizationName = xyz
organizationalUnitName = xyz
commonName = abc
emailAddress = test@blackbox.com
```

Download CSR Delete CSR

SSL Certificate Upload

SSL Certificate File Browse...

Upload

Figure 5.31: SSL Certificate Signing Request

use WinZip from <http://www.winzip.com/> for uncompression. Other operating systems might provide a program called unzip.

Before you can start updating the firmware of your RAS-PutIn the new uncompressed firmware file must be accessible on the system that you use for connecting to RAS-PutIn.

Updating the firmware is a three-stage process:

- Firstly the new firmware file is uploaded onto RAS-PutIn. In order to do that you need to select the file on your local system using the browse button of the Upload Firmware panel (see Figure 5.32 on the next page). Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted.



Upload Firmware

Firmware File Browse...

Upload

Figure 5.32: Panel for uploading a new firmware

- Secondly, if everything went well, you see the Update Firmware panel (see Figure 5.33 on the following page). The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the update button will store the new version over the old one. Attention: this process is not reversible and might take some minutes. Make sure the RAS-PutIn's power supply won't be interrupted during the update process, because this may cause an unusable device.
- Thirdly, after the firmware has been stored, the panel will request you to reset RAS-PutIn manually. Half a minute after the reset, RAS-PutIn will run with the new firmware version and should be accessible. However, you are requested to login once again.

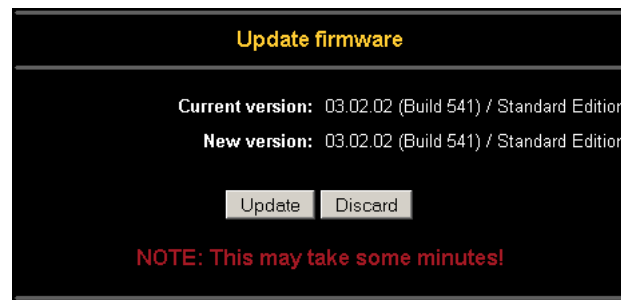


Figure 5.33: Panel to update a new firmware that was previously uploaded

Attention:

The three-stage firmware update process and complete consistency check are making a mistake in updating the firmware almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure RAS-PutIn's power supply won't be interrupted!

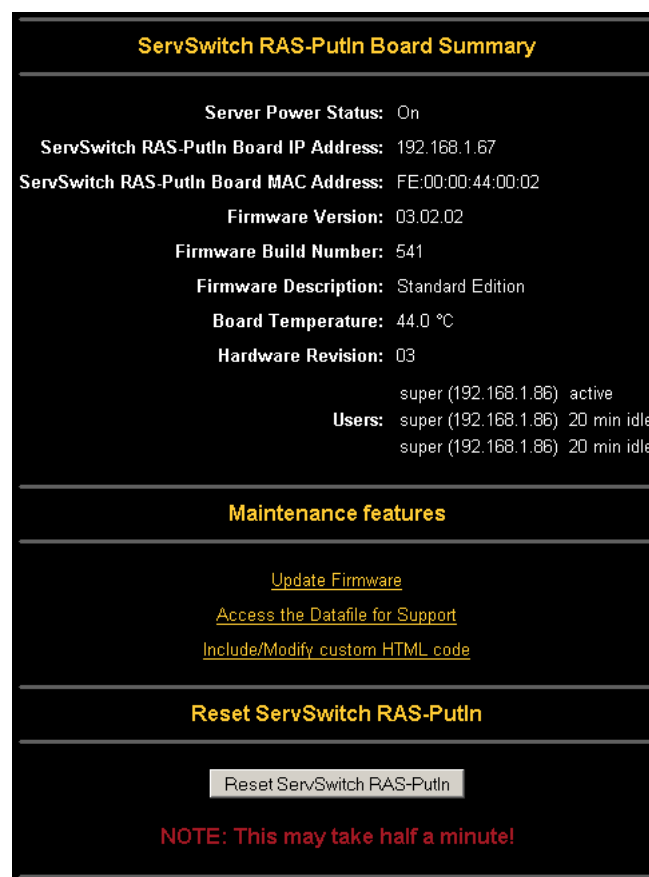


Figure 5.34: Maintenance

5.6 Access via Telnet

The RAS-PutIn firmware features a Telnet server that enables a user to connect via a standard Telnet client. It is used for passthrough access to a device possibly connected to the serial port

1. This means you may connect any serial device which offers terminal access via its serial port to RAS-PutIn and access it using the Telnet interface. Set the serial settings (see Section 5.5.5 on page 47) according to the requirements of the device.

Connecting to RAS-PutIn is done as usual and as required by the Telnet client, for instance in a UNIX shell:

```
telnet 192.168.1.226
```

This will prompt for username and password in order to log into the card. The credentials that need to be entered for authentication are identical to those of the Web interface. That means, the user management of the Telnet interface is entirely controlled with the according functions of the Web interface.

Once you have successfully logged in RAS-PutIn will present you the command line where you can enter according management commands.

In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were made accordingly). All inputs are redirected to the device on serial port 1 and its answers are displayed at the Telnet interface

The following list shows the according command mode command syntax and their usage.

- **help**
Shows the list of the following commands
- **cls**
Clear screen
- **logout**
Logs out the current user and disconnects from the client
- **version**
Shows a compound string off all available version numbers
- **terminal**
Starts the terminal passthrough mode for serial port 1. The key sequence ‘<esc> exit’ switches back to command modus.

⁶The IP address has to be replaced by the one that is actually assigned to RAS-PutIn.

6 Frequently Asked Questions

Q 001: The remote mouse doesn't work or is not synchronous

A 001: Make sure the mouse settings in RAS-PutIn match the mouse model. There are some circumstances where the mouse synchronization process could behave incorrectly, refer to Section 5.3.3 on page 27 for further explanation.

Q 002: The video quality is bad or the picture is grainy

A 002: Try to correct the brightness and contrast settings (see Section 5.3.4 on page 28) until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.

Q 003: Login on RAS-PutIn fails.

A 003: Was the correct combination of user and password given? On delivery, the user "super" has the password "rasputin". Moreover your browser must be configured to accept cookies.

Q 004: The Remote Console window can't connect to RAS-PutIn.

A 004: Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connection establishments.

Q 005: No connection can be established to RAS-PutIn.

A 005: Check whether the network connection is working in general (ping the IP address of RAS-PutIn). If not, check network hardware. Is RAS-PutIn powered on? Check whether the IP address of RAS-PutIn and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, like routers etc., are correctly configured. Without a ping functioning, RAS-PutIn can't work either.

Q 006: Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.

A 006: You have to define a so-called 'Button Key'. This can be done in the Remote Console settings.

Q 007: In the browser the RAS-PutIn pages are inconsistent or chaotic.

A 007: Make sure your browser cache settings are feasible. Especially make sure the cache settings are not set to something like "never check for newer pages". Otherwise RAS-PutIn pages may be loaded from your browser cache and not from the card.

Q 008: Windows XP doesn't awake from standby mode

A 008: This is possibly a Windows XP problem. Try not to move the mouse while XP goes in standby mode.

Q 009: Using MacOS X a HTTPS connection fails

A 009: You have to install the Blackbox certificate using our certificate installer, available on the utility CD. Please refer to the instructions on this CD for further information how to install the certificate.

Q 010: Can't upload the signed certificate in MacOS X

A 010: If an 'internal error' occurs while uploading the signed certificate either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is plain text and the checkbox 'use for outgoing' is checked. Another possibility is to use a Mozilla based browser.

Q 011: Everytime I open a dialog box with some buttons the mouse pointers are not synchronous anymore

A 011: Please check, if you have an option like "Automatically move mouse pointer to the default button of dialog boxes" enabled in the mouse settings of the operating system. This option needs to be disabled.

A Glossary

ACPI	A specification that enables the operating system to implement power management and system configuration.
ATX	Advanced Technology Extended: A particular specification of a motherboard introduced by Intel in 1995.
BMC	Board Management Controller: implements the IPMI based main board management functions.
DHCP	Dynamic Host Configuration Protocol: protocol for dynamically assigning IP configurations in local networks.
DNS	Domain Name System: protocol used to locate computers on the Internet by their name.
EMP	Emergency Management Port: provides remote emergency access and control of server resources. EMP offers operating system independent, fundamental remote management access regardless of the server's current state or network availability.
FAQ	Frequently Asked Questions
HTTP	Hypertext Transfer Protocol: the protocol used between web browsers and servers.
HTTPS	Hyper Text Transfer Protocol Secure: secure version of HTTP.
IPMI	Intelligent Platform Management Interface
LED	Light Emitting Diode
MIB	Management Information Base: describes the structure of the management information that can be accessed via SNMP.
PS/2	The PS/2 device interface was developed by IBM and is used by many mice and keyboards.
SNMP	Simple Network Management Protocol: a widely used network monitoring and control protocol.
SSL	Secure Socket Layer: encryption technology for the Internet used to provide secured data transmissions.
SVGA	Super VGA: A refinement of Video Graphics Array (VGA) that provides increased pitch and resolution performance.
UTP	Unshielded Twisted Pair: a cable with two conductors twisted as a pair and bundled within the same outer PVC covering.

B RAS-PutIn Video Modes

Table B.1 lists the video modes RAS-PutIn supports. Please don't use other custom video settings besides of these. If done so, RAS-PutIn may not be able to detect them.

Table B.1: RAS-PutIn Video Modes

Resolution (x,y)	Refresh Rates (Hz)
640x350	70, 85
640x400	56, 70, 85
640x480	60, 67, 72, 75, 85, 90, 100, 120
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85, 90, 100
832x624	75
1024x768	60, 70, 72, 75, 85, 90, 100
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60
1280x1024	60

C Key Codes

Table C.1 shows the key codes used to defines key strokes or hotkeys for several functions. Please note that these key codes do not represent necessarily key characters that are used on international keyboards. They name a key on a standard 104 key PC keyboard with an US English language mapping. The layout for this keyboard is shown in Figure C.1. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are on an identical position, no matter what language mapping you are using. Some of the keys have aliases also, means they can be named by 2 key codes (separated by comma in the table).

Esc	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	Prnt	Scrl	Brk						
~	1	2	3	4	5	6	7	8	9	0	-	=	Bsp	Ins	Pos1	Pgup	Num	/	*	-	
tab	q	w	e	r	t	y	u	i	o	p	[]	CR	Del	End	Pgdn	7	8	9	+	
Caps	a	s	d	f	g	h	j	k	l	;	'	\						4	5		6
LShift	z	x	c	v	b	n	m	,	.	?	Rshift				Up		1	2	3	CR	
Lctrl	Win	Alt	Space					AltGR	Menu	RCtrl	Left	Down	Right	0	,						

Figure C.1: English (US) Keyboard Layout, used for key codes

Table C.1: Key Names

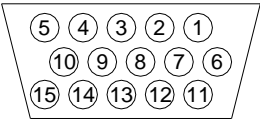
Key (and aliases)
0 - 9
A - Z
, TILDE
-, MINUS
=, EQUALS
;
<, LESS
,
.
/, SLASH
BACK_SPACE
TAB
[
]
ENTER
CAPS_LOCK
\, BACK_SLASH
LSHIFT, SHIFT
Continued on next page

Table C.1 – continued from previous page

Key (and aliases)
RCTRL
RSHIFT
LCTRL, CTRL
LALT, ALT
SPACE
ALTGR
ESCAPE, ESC
F1
F2
F3
F4
F5
F6
F7
F8
F9
F10
F11
F12
PRINTSCREEN
SCROLL_LOCK
BREAK
INSERT
HOME
PAGE_UP
DELETE
END
PAGE_DOWN
UP
LEFT
DOWN
RIGHT
NUM_LOCK
NUMPAD0
NUMPAD1
NUMPAD2
NUMPAD3
NUMPAD4
NUMPAD5
NUMPAD6
NUMPAD7
NUMPAD8
NUMPAD9
NUMPADPLUS,NUMPAD_PLUS
NUMPAD/
NUMPADMUL,NUMPAD_MUL
NUMPADMINUS,NUMPAD_MINUS
NUMPADENTER
WINDOWS
MENU

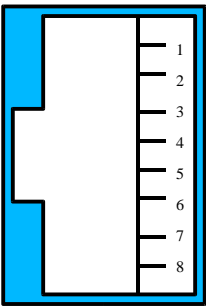
D Pin Assignments

D.1 VGA HD-15



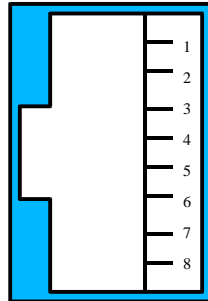
Pin	Assignment	Pin	Assignment
1	Red	9	5 V
2	Green	10	GND sync
3	Blue	11	Not connected
4	Not connected	12	SDA, DDC, ...
5	GND	13	HSYNC
6	GND red	14	VSYNC
7	GND green	15	DATA_CLOCK
8	GND blue		

D.2 RJ 45 Connector Ethernet



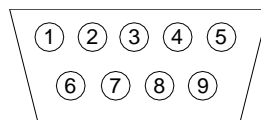
Pin	Assignment	Pin	Assignment
1	TX +	5	Not connected
2	TX -	6	RX -
3	RX +	7	Not connected
4	Not connected	8	Not connected

D.3 RJ 45 Connector ISDN



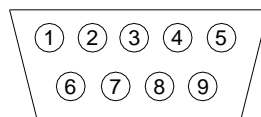
Pin	Assignment	Pin	Assignment
1	Not connected	5	RX -
2	Not connected	6	TX -
3	TX +	7	Not connected
4	RX +	8	Not connected

D.4 Serial SUB-D 9 Connector 1



Pin	Assignment	Pin	Assignment
1	DCD	6	DSR
2	RX	7	RTS
3	TX	8	CTS
4	DTR	9	RI
5	GND		

D.5 Serial SUB-D 9 Connector 2



Pin	Assignment	Pin	Assignment
1	DCD	6	DSR, Reset2
2	RX	7	RTS, Power1
3	TX	8	DTS, Power2
4	DTR, Reset1	9	Not connected
5	GND		

Pins 1 and 6 are bridged

D.6 KVM SUB-D 25 Connector

①

②

③

④

⑤

⑥

⑦

⑧

⑨

⑩

⑪

⑫

⑬

⑭

⑮

⑯

⑰

⑱

⑲

⑳

㉑

㉒

㉓

㉔

㉕

Pin	Assignment	Pin	Assignment
1	VGA blue	14	GND
2	VGA green	15	GND
3	VGA red	16	GND
4	VGA hsync	17	VGA vsync
5	GND	18	Not connected
6	VGA SCL	19	VGA SCL
7	GND	20	GND
8	Not connected	21	GND
9	KBD data	22	KBD clock
10	GND	23	RS232 2 TX
11	MOUSE clock	24	RS232 2 RX
12	MOUSE data	25	MOUSE +5V
13	KBD +5V		

D.7 Power Supply Connector

①

②

③

④

Pin	Assignment
1	+12V
2	+12V
3	GND
4	GND

E Blackbox Warranty information

LIMITED WARRANTY

Blackbox manufactures its hardware products from parts and components that are new or equivalent to new in accordance with industry-standard practices. Blackbox warrants that the hardware products including the firmware will be free from defects in materials and workmanship under normal use. Any implied warranties on the Blackbox firmware and hardware are limited to 24 months, respectively, beginning on the date of invoice. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES

Blackbox's entire liability and exclusive remedy shall be, at Blackbox's option, either (a) return of the price paid, or (b) repair or replacement of the firmware or hardware that does not meet this Limited Warranty and which is returned to Blackbox with a copy of your receipt. Damage due to shipping the products to you is covered under this warranty. Otherwise warranty does not cover damage due to external causes, including accident, abuse, misuse, problems with electrical power, servicing not authorized by Blackbox, usage not in accordance with product instructions, failure to perform required preventive maintenance and problems caused by use of parts and components not supplied by Blackbox. Any replacement hardware will be warranted for the remainder of the original period or thirty (30) days, whichever is longer.

Blackbox will repair or replace products returned to Blackbox's facility. To request warranty service you must inform Blackbox within the warranty period. If warranty service is required, Blackbox will issue a Return Material Authorization Number. You must ship the products back to Blackbox in their original or an equivalent packaging, prepay shipping charges, and insure the shipment or accept the possibility of loss or damage during shipment.

NO OTHER WARRANTIES

To the maximum extent permitted by applicable law, Blackbox disclaim all other warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose, with regard to the firmware, the accompanying written materials, and any accompanying hardware. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES

To the maximum extent permitted by applicable law, in no event shall Blackbox be liable for any damages whatsoever (including without limitation, special, incidental, consequential or indirect damages for personal injury, loss of business information, or any other pecuniary loss)

arising out of the use of or inability to use this product, even if Blackbox has been advised of the possibility of such damages. In any case, Blackbox entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the firmware and/or hardware. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

F Specifications

F.1 Size and Weight

Height:	44 mm 1 HU (Height Unit)
Width:	105 mm 1/4 19"
Length (Box):	223 mm
Length (Box with connectors):	233
Weigh:	700 g

F.2 Environmental

Temperature	
Operating	0°C to 40°C (32°F to 131°F)
Storage	-18°C to 70°C (-20°F to 158°F)
Humidity:	
Operating	10% to 90% (non-condensing)
Storage	5% to 95% (non-condensing)

G Operation advices

- This device has to be operated with the provided power supply 'BLACKBOX ENG/EPA-121DA-12' only. Use of other power supplies voids the product liability of the manufacturer. If the power supply shows a malfunction, it must not be opened. Instead a replacement has to be requested from the manufacturer or the vender.
- The power cord of the power supply is the point of junction to the supply network AC 230 V. Therefore the power supply and socket have to be easily accessible to disconnect them quickly if it is necessary.
- The device contains a lithium battery CR 1632. Gladly we exchange this battery for you. When changing the battery yourself, please notice: 'Attention, explosion hazard while exchanging the battery improperly. Disposal of old batteries has to be done as mentioned on the package of the new one.'